# Symmetric Boolean functions

Anne Canteaut, Marion Videau

# Symmetric Boolean Functions

Anne Canteaut and Marion Videau

***Abstract*—We present an extensive study of symmetric Boolean functions, especially of their cryptographic properties. Our main result establishes the link between the periodicity of the simplified value vector of a symmetric Boolean function and its degree. Besides the reduction of the amount of memory required for representing a symmetric function, this property has some consequences from a cryptographic point of view. For instance, it leads to a new general bound on the order of resiliency of symmetric functions, which improves Siegenthaler's bound. The propagation characteristics of these functions are also addressed and the algebraic normal forms of all their derivatives are given. We finally detail the characteristics of the symmetric functions of degree at most 7, for any number of variables. Most notably, we determine all balanced symmetric functions of degree less than or equal to 7.**

***Index Terms*—Boolean functions, correlation immunity, degree, derivation, propagation criterion, resiliency, symmetric functions.**

## I. Introduction

SYMMETRIC Boolean functions are characterized by the fact that their outputs only depend on the Hamming weights of their inputs. These functions can be represented in a very compact way both for their algebraic normal forms and for their value vectors. This property is useful: for instance, a Boolean function of more than 15 variables can be used practically as a filtering function in a stream cipher only if it can be represented in a concise form. As symmetric functions are the only functions having a known implementation with a number of gates which is linear in the number of input variables [1], they might be good candidates in term of implementation complexity. On the other hand, the fact that a symmetric Boolean function can be entirely described by an $(n+1)$-bit vector considerably reduces the amount of memory required for storing the function and is of great interest in software applications.

However, the usefulness of symmetric functions in a cryptographic context (e.g., in stream ciphers, block ciphers, or hash functions) needs to be clarified: symmetric functions which possess good cryptographic properties have not yet been exhibited.

Starting from a suggestion of Brüer [2] who stressed the importance of not having any input of greater or lesser significance than any other input, the property of symmetry was investigated in a systematic way among other cryptographically significant properties of functions in [3] and [4]. The aim was to check that a sufficient amount of good functions could fulfill all the requirements. The property of symmetry was suspected to be overrestrictive.

It is known that the algebraic degree and the nonlinearity, which are two important cryptographic parameters, cannot be simultaneously maximized for symmetric functions. Most notably, it was proved in [5] and [6] that the highest possible nonlinearity for a symmetric function is only achieved by quadratic functions. However, symmetric functions with suboptimal nonlinearity might exist and might be of interest for designing fast cryptographic primitives. Besides the Hamming distance to linear functions, some other criteria, such as correlation immunity or propagation characteristics, are required in some applications and need to be addressed in the context of symmetric functions. The existence of correlation-immune and resilient symmetric functions has been investigated in [7]–[9]. For instance, a few infinite families of 1– or 2-resilient symmetric functions have been exhibited, but there is a lack of general results on the order of resiliency of symmetric functions. The conjecture [8] which states that the affine functions are the only 3-resilient symmetric functions remains open.

The present work establishes some general properties of symmetric functions related to the previously mentioned cryptographic criteria. Most of the obtained results are based on a theorem presented in Section III which shows that the algebraic degree of a symmetric function is characterized by the period of the corresponding simplified value vector. This property has two major consequences. From a practical point of view, it enables to shorten the vector used for representing a low-degree symmetric function, since any symmetric function of degree $d$ can be completely described by a $2^{\lfloor \log_2 d \rfloor + 1}$-bit vector. Additionally, the link between the degree and the periodicity of the simplified value vector leads to general results on the cryptographic properties of symmetric functions. For instance, we prove in Section IV that the order of resiliency of a symmetric function of degree $d$ cannot exceed $\left(2^{\lfloor \log_2 d \rfloor + 1} - 2\right)$. This new bound provides a general improvement of Siegenthaler's bound for symmetric functions for large values of $n$, precisely as soon as $n$ is greater than $2^{\lfloor \log_2 d \rfloor + 1} + d - 1$. Section V focuses on the propagation characteristics of symmetric functions. Most notably, we are able to provide the general expression of the algebraic normal forms of all the derivatives of a symmetric function. Section VI is devoted to an extensive study of all characteristics (weight, Walsh coefficients, weights of derivatives) of the symmetric functions of degree less than or equal to 7. We notably determine all balanced symmetric functions of degree at most 7 for any number of variables. Finally, in the last section, we link the nonlinearity of a symmetric Boolean function to the periodicity of its simplified value vector and investigate the cases of suboptimal nonlinearity.

Manuscript received May 27, 2004; revised April 11, 2005. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004.

The authors are with the INRIA–Projet CODES, B.P. 105, 78153 Le Chesnay Cedex, France (e-mail: anne.canteaut@inria.fr; marion.videau@inria.fr).

Communicated by T. Johansson, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2005.851743

## II. Basic Properties of Symmetric Functions

### A. Notation

We first recall some general properties of Boolean functions (see, e.g., [10]). Let $\boldsymbol{F}_2$ denote the finite field with two elements. To prevent confusion with the usual sum, we denote by $\oplus$ the sum over $\boldsymbol{F}_2$. The *Hamming weight* of a binary vector $v = (v_1, \ldots, v_n)$, is defined by $\mathrm{wt}(v) = \sum_{i=1}^{n} v_i$.

We denote by $\mathcal{B}_n$ the set of all Boolean functions of $n$ variables, i.e., of all the functions from $\boldsymbol{F}_2^n$ into $\boldsymbol{F}_2$. Any $f \in \mathcal{B}_n$ can be expressed as a polynomial, called its algebraic normal form (ANF)

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \boldsymbol{F}_2^n} \lambda_u \left( \prod_{i=1}^{n} x_i^{u_i} \right), \qquad \lambda_u \in \boldsymbol{F}_2$$

with

$$\lambda_u = \bigoplus_{x \preceq u} f(x)$$

where $(x_1, \ldots, x_n) \preceq (u_1, \ldots, u_n)$ if and only if $\forall\, i,\ x_i \leq u_i$. The *degree* of $f$, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $\lambda_u \neq 0$.

Any function in $\mathcal{B}_n$ can also be identified with the binary vector of length $2^n$ consisting of all values $f(x)$, $x \in \boldsymbol{F}_2^n$ (the order of the elements in $\boldsymbol{F}_2^n$ is fixed and will be the same in the remainder of the paper, it will not influence the results). By convention, the weight of $f$ is the weight of this vector and will be denoted by $\mathrm{wt}(f)$.

For any $a \in \boldsymbol{F}_2^n$, $\varphi_a$ will denote the linear function in $\mathcal{B}_n$ : $x \mapsto a \cdot x$, where $x \cdot y$ is the usual dot product between two vectors. For any $f \in \mathcal{B}_n$, we denote by $\mathcal{F}(f)$ the following value related to the Walsh (or Fourier) transform of $f$

$$\mathcal{F}(f) = \sum_{x \in \boldsymbol{F}_2^n} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f).$$

The function is said to be *balanced* if $\mathrm{wt}(f) = 2^{n-1}$ or, equivalently, $\mathcal{F}(f) = 0$.

*Definition 1:* The Walsh (or Fourier) coefficient of $f \in \mathcal{B}_n$ in point $a \in \boldsymbol{F}_2^n$ corresponds to

$$\mathcal{F}(f + \varphi_a) = \sum_{x \in \boldsymbol{F}_2^n} (-1)^{f(x) + a \cdot x}.$$

The values of the Walsh coefficients $\mathcal{F}(f + \varphi_a)$, $a \in \boldsymbol{F}_2^n$ form the *Walsh spectrum* of $f$.

The *nonlinearity* $\mathcal{N}_f$ of $f$ is the Hamming distance between $f$ and the set of affine functions. It is related to the Walsh transform via the following expression:

$$\mathcal{N}_f = 2^{n-1} - \frac{\mathcal{L}(f)}{2}, \quad \text{where } \mathcal{L}(f) = \max_{a \in \boldsymbol{F}_2^n} \left| \mathcal{F}(f + \varphi_a) \right|.$$

High nonlinearity is an important cryptographic criterion since the existence of a good linear approximation should be avoided in most applications (see, e.g., [11]). When $n$ is even, it is known that $\mathcal{L}(f) \geq 2^{n/2}$ with equality for functions whose Walsh coefficients take the two values $\pm 2^{n/2}$ only—the so-called bent functions [12]. When $n$ is odd, any $f$ satisfies $\mathcal{L}(f) > 2^{\frac{n}{2}}$. For odd $n < 9$, $\mathcal{L}(f) \geq 2^{(n+1)/2}$ where equality holds for the so-called almost optimal functions (see [10, Definition V.1]).

Some other cryptographic criteria are related to the propagation characteristics of Boolean functions. They focus on the properties of their derivatives.

*Definition 2:* Let $f \in \mathcal{B}_n$. The derivative of $f$ with respect to $a \in \boldsymbol{F}_2^n$ is the function $D_a f \in \mathcal{B}_n$ defined by

$$D_a f(x) = f(x + a) \oplus f(x).$$

Any nonzero $a \in \boldsymbol{F}_2^n$ such that $D_a f$ is a constant function is said to be a linear structure for $f$.

### B. Symmetric Functions

Now, we focus on the particular family of symmetric Boolean functions.

*Definition 3:* A Boolean function is said to be symmetric if its output is invariant under any permutation of its input bits. For a symmetric Boolean function $f$ of $n$ variables, we have

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

for all permutations $\sigma$ of $\{1, \ldots, n\}$.

This equivalently means that the output of $f$ only depends on the weight of its input vector. As a consequence, $f$ is related to a function $v_f : \{0, \ldots, n\} \to \boldsymbol{F}_2$ such that $\forall\, x \in \boldsymbol{F}_2^n$, $f(x) = v_f(\mathrm{wt}(x))$. We will consider the sequence $v(f) = (v_f(0), \ldots, v_f(n))$ and refer to it as the simplified value vector of $f$.

*Proposition 1:* A Boolean function $f$ of $n$ variables is symmetric if and only if its algebraic normal form can be written as follows:

$$\begin{aligned} f(x_1, \ldots, x_n) &= \bigoplus_{i=0}^{n} \lambda_f(i) \bigoplus_{\substack{u \in \boldsymbol{F}_2^n \\ \mathrm{wt}(u) = i}} \left( \prod_{j=1}^{n} x_j^{u_j} \right) \\ &= \bigoplus_{i=0}^{n} \lambda_f(i) X_{i,n}, \quad \lambda_f(i) \in \boldsymbol{F}_2^n, \end{aligned}$$

where $X_{i,n}$ is the elementary symmetric polynomial of degree $i$ in $n$ variables.

Then, the coefficients of the ANF of $f$ can be represented by the $(n+1)$-bit vector, $\lambda(f) = (\lambda_f(0), \lambda_f(1), \ldots, \lambda_f(n))$, called the simplified ANF vector of $f$.

The following proposition establishes the relationship between the simplified ANF vector and the simplified value vector of a symmetric Boolean function. It generalizes [6, Theorem 3].

*Proposition 2:* Let $f$ be a symmetric Boolean function of $n$ variables. Then, its simplified value vector $v(f)$ and its simplified ANF vector $\lambda(f)$ are related by

$$\forall\, i \in \{0, \ldots, n\}, \quad v_f(i) = \bigoplus_{k \preceq i} \lambda_f(k) \text{ and } \lambda_f(i) = \bigoplus_{k \preceq i} v_f(k).$$

*Proof:* Let $f(x_1, \ldots, x_n) = \bigoplus_{i=0}^{n} \lambda_f(i) X_{i,n}$. For a given $x$ of weight $k$, $X_{i,n}$ contains $\binom{i}{k}$ nonzero monomials. The expression of binomial coefficients modulo a prime number $p$ is

given by Lucas' theorem (e.g., [13, p. 79]). Given two integers $a$ and $b$ and their $p$-adic representations $a = \sum_{i=0}^{e} a_i p^i$ and $b = \sum_{i=0}^{e} b_i p^i$, we have

$$\binom{a}{b} \equiv \prod_{i=0}^{e} \binom{a_i}{b_i} \bmod p.$$

For $p = 2$, we obtain

$$\binom{a}{b} \equiv 1 \mod 2 \text{ if and only if } \mathrm{supp}(b) \subseteq \mathrm{supp}(a)$$

i.e., $b \preceq a$ which means that $\forall\, i,\ b_i \leq a_i$. We finally get

$$v_f(i) = \bigoplus_{k=0}^{i} \binom{i}{k} \lambda_f(k) = \bigoplus_{k \preceq i} \lambda_f(k).$$

Conversely, the coefficients of the algebraic normal form of $f$ can be computed from its simplified value vector

$$\forall\, u \in \boldsymbol{F}_2^n, \quad \lambda_u = \bigoplus_{x \preceq u} f(x).$$

This can be written as

$$\lambda_u = \bigoplus_{k=0}^{\mathrm{wt}(u)} \binom{\mathrm{wt}(u)}{k} v_f(k).$$

We can notice that $\lambda_u$ only depends on the weight of $u$. Then, for $\mathrm{wt}(u) = i$, Lucas' theorem leads to

$$\lambda_f(i) = \bigoplus_{k=0}^{i} \binom{i}{k} v_f(k) = \bigoplus_{k \preceq i} v_f(k). \qquad \square$$

Symmetric Boolean functions are also characterized by the symmetry of their Walsh transform.

*Proposition 3 [5], [14]:* A Boolean function is symmetric if and only if its Walsh transform is a real-valued symmetric function. Moreover, the Walsh coefficients of a symmetric function $f \in \mathcal{B}_n$ are given by

$$\forall\, a \in \boldsymbol{F}_2^n, \quad \mathcal{F}(f + \varphi_a) = \sum_{w=0}^{n} (-1)^{v_w} P_w(\mathrm{wt}(a))$$

where $P_w$ is the Krawtchouk polynomial of degree $w$, i.e.,

$$P_w(i) = \sum_{k=0}^{w} \binom{i}{k} \binom{n-i}{w-k} (-1)^k.$$

## III. Regular Patterns in the Simplified Value Vector

Here, we show that some cryptographic properties, such as the degree or the balancedness of a symmetric function, are characterized by the existence of regular patterns in the corresponding simplified value vector.

### A. Periodicity of the Simplified Value Vector

We first focus on the periodicity of the simplified value vector. Let $a = (a_n)_{n \in \boldsymbol{N}}$ be an infinite binary sequence. We say that $a$ is periodic with period $T$ if $a_{n+T} = a_n$ for all $n \in \boldsymbol{N}$. For $a_0, \ldots, a_{T-1} \in \boldsymbol{F}_2$, we denote by $(a_0, \ldots, a_{T-1})^*$ the infinite periodic sequence $u = (u_n)_{n \in \boldsymbol{N}}$, $u_n \in \{0, 1\}$ with period $T$ defined by

$$\begin{cases} u_i = a_i, & \text{if } 0 \leq i \leq T-1 \\ u_{T+i} = u_i, & \forall\, i \in \boldsymbol{N}. \end{cases}$$

*Definition 4:* An $n$-bit vector $(v_0, \ldots, v_{n-1})$ is said to be a part of an infinite sequence if it is composed of the first $n$ values of this infinite sequence. Moreover, we say that the $n$-bit vector $(v_0, \ldots, v_{n-1})$ is periodic with period $T < n$ if it is a part of the infinite periodic sequence $(v_0, \ldots, v_{T-1})^*$.

It was shown in [6, Theorem 5] that, for any odd $n$, the quadratic symmetric functions of $n$ variables are the functions whose simplified value vectors are parts of either $(0011)^*$, $(0110)^*$, $(1100)^*$, or $(1001)^*$. Here, we prove that the degree of a symmetric function is characterized by the periodicity of its simplified value vector.

*Theorem 1:* Let $f \in \mathcal{B}_n$ be a symmetric function with simplified ANF vector $\lambda(f) = (\lambda_0, \ldots, \lambda_n)$ and simplified value vector $v(f) = (v_0, \ldots, v_n)$.

Then, $v(f)$ is periodic with period $2^t$, $2^t < n$, if and only if $\deg(f) \leq 2^t - 1$. Moreover, $(v_0, \ldots, v_{2^t-1})$ is the simplified value vector of the symmetric Boolean function of $(2^t - 1)$ variables with $(\lambda_0, \ldots, \lambda_{2^t-1})$ as simplified ANF vector.

*Proof:* We decompose any integer $i \leq n$ as $i = i_2 2^t + i_1$ with $i_1 \leq 2^t - 1$. Proposition 2 leads to

$$\begin{aligned} \lambda_{i_2 2^t + i_1} &= \bigoplus_{k \preceq i_2 2^t + i_1} v_k \\ &= \bigoplus_{k_2 \preceq i_2} \bigoplus_{k_1 \preceq i_1} v_{k_2 2^t + k_1} \\ &= \bigoplus_{k_2 \preceq i_2} \bigoplus_{k_1 \preceq i_1} v_{k_1} \\ &= 2^{\mathrm{wt}(i_2)} \bigoplus_{k_1 \preceq i_1} v_{k_1} \end{aligned}$$

which implies that $\lambda_{i_2 2^t + i_1} = 0$ for all nonzero $i_2$ (i.e., that $\deg(f) < 2^t$)). Moreover, the first coefficients of the simplified ANF vector $(\lambda_0, \ldots, \lambda_{2^t-1})$ exactly correspond to the simplified ANF vector of the symmetric Boolean function of $(2^t - 1)$ variables with simplified value vector $(v_0, \ldots v_{2^t-1})$.

The converse can be proved by similar calculations. Let $f \in \mathcal{B}_n$ be a symmetric function with $\deg(f) \leq 2^t - 1$. Then, for $i = i_2 2^t + i_1$ with $i_1 < 2^t$, we have

$$v_{i_2 2^t + i_1} = \bigoplus_{k \preceq i_2 2^t + i_1} \lambda_k = \bigoplus_{k \preceq i_1} \lambda_k = v_{i_1}.$$

It follows that the simplified value vector of $f$ is periodic with period $2^t$, and that its first $2^t$ terms correspond to the simplified value vector of the symmetric Boolean function of $(2^t - 1)$ variables with simplified ANF vector $(\lambda_0, \ldots \lambda_{2^t-1})$. $\square$

For symmetric functions of degree exactly $2^t$, we can precise the previous result.

*Proposition 4:* Let $f \in \mathcal{B}_n$ be a symmetric function. Then, $\deg(f) = 2^t$ if and only if $v(f)$ is periodic with period $2^{t+1}$ and is a part of $(v_0, \ldots, v_{2^t-1}, v_0 \oplus 1, \ldots, v_{2^t-1} \oplus 1)^*$.

*Proof:* The calculations are based on the same principles as above. Here, we use that, for all $i > 2^t$, $\lambda_i = 0$ and $\lambda_{2^t} = 1$. Then, we have

$$\begin{aligned} v_{i_2 2^t + i_1} &= \bigoplus_{k \preceq i_2 2^t + i_1} \lambda_k \\ &= \bigoplus_{k_2 \preceq i_2} \bigoplus_{k_1 \preceq i_1} \lambda_{k_2 2^t + k_1} \\ &= v_{i_1} \oplus (i_2 \bmod 2). \end{aligned}$$

Conversely, we can determine the degree of $f$ if $v(f)$ is a part of $(v_0, \ldots, v_{2^t-1}, v_0 \oplus 1, \ldots, v_{2^t-1} \oplus 1)^*$. We have for all $i < 2^t$

$$\begin{aligned}\lambda_{2^t+i} &= \bigoplus_{k \preceq 2^t+i} v_k \\ &= \bigoplus_{k_2 \preceq 1} \bigoplus_{k_1 \preceq i} v_{k_2 2^t + k_1} \\ &= \bigoplus_{k_1 \preceq i} (v_{k_1} \oplus v_{2^t+k_1}) \\ &= \bigoplus_{k_1 \preceq i} 1 = 2^{\mathrm{wt}(i)} \bmod 2\end{aligned}$$

which is equal to zero except for $i = 0$. □

Both previous properties are of great interest since they significantly reduce the amount of memory required for storing an $n$-variable function of degree $d$ when $n \geq 2^{\lfloor \log_2 d \rfloor + 1}$. The first $2^{\lfloor \log_2 d \rfloor + 1}$ bits of its simplified value vector together with the $(\lfloor \log_2 n \rfloor + 1)$ bits of the representation of $n$ actually provide a complete description of the function instead of the $(n+1)$-bit vector previously needed. It means, for example, that for a 64-variable symmetric Boolean function of degree 15, 22 bits are needed to represent the function instead of 65 bits.

The relationship between the degree of a symmetric function and the periodicity of its simplified value vector has many other consequences, especially on the cryptographic properties of symmetric functions. It will be extensively used in the following sections, especially for computing the Hamming weights or studying the resiliency orders of low-degree symmetric functions.

### B. Trivial Balanced Functions

Now, we focus on another particular pattern which may occur in the simplified value vectors of some symmetric functions depending on an odd number of variables.

*Definition 5:* Let $n$ be an odd integer and $f \in \mathcal{B}_n$ be a symmetric function. We say that $f$ is a trivial balanced function if

$$\forall\, 0 \leq i \leq n, \qquad v_f(i) = v_f(n-i) \oplus 1.$$

It is obvious that symmetric functions having this property are balanced because of the symmetry of binomial coefficients for odd $n$. Trivial balanced functions exactly correspond to symmetric functions $f$ which verify $D_{\mathbf{1}} f = 1$, where $\mathbf{1}$ denotes the all-one vector. Indeed, functions with $D_{\mathbf{1}} f = 1$ do not exist for even values of $n$ because, for any vector $u$ such that $\mathrm{wt}(u) = n/2$, we have

$$D_{\mathbf{1}} f = f(u) \oplus f(u+\mathbf{1}) = v_f(n/2) \oplus v_f(n/2) = 0.$$

Trivial balanced functions also correspond to the odd case of the trivial partitioning in [3, Theorem 3.6.5]. The even case corresponds to affine functions. Finding partitions of the set of the $n$ binomial coefficients leading to balanced symmetric Boolean functions is, in fact, equivalent to finding patterns of the simplified value vector of balanced symmetric Boolean functions.

Trivial balanced functions can be characterized by the following equivalent properties.

*Proposition 5:* Let $n$ be an odd integer and $f \in \mathcal{B}_n$ be a symmetric function. The following properties are equivalent.

i) For all $i$, $0 \leq i \leq n$, $v_f(i) = v_f(n-i) \oplus 1$.
ii) The derivative of $f$ with respect to the all-one vector $\mathbf{1}$ is the constant function 1.
iii) For all $a \in \boldsymbol{F}_2^n$ such that $\mathrm{wt}(a)$ is even, $\mathcal{F}(f+\varphi_a) = 0$.
iv) For all $a \in \boldsymbol{F}_2^n$, $D_{a+\mathbf{1}} f = D_a f + 1$, hence,

$$\mathcal{F}(D_{a+\mathbf{1}} f) = -\mathcal{F}(D_a f).$$

*Proof:* We show that Properties ii) and iii) are equivalent. Let $H_{\mathbf{1}}$ be the hyperplane $\{0, \mathbf{1}\}^{\perp}$, composed of all the words of even weight. According to [10, Lemma V.2], we have

$$\sum_{a \in H_1} \mathcal{F}^2(f+\varphi_a) = 2^{n-1}(\mathcal{F}(D_0 f) + \mathcal{F}(D_{\mathbf{1}} f)).$$

Therefore, $\mathcal{F}(D_{\mathbf{1}} f) = -2^n$ if and only if $\mathcal{F}(f+\varphi_a) = 0$, $\forall\, a \in H_{\mathbf{1}}$.

We now show that ii) and iv) are equivalent. It is well known that, for any $f \in \mathcal{B}_n$ and any $a, b \in \boldsymbol{F}_2^n$, we have

$$D_{a+b} f = D_a f + D_b f + D_a D_b f.$$

For $b = \mathbf{1}$, we obtain

$$\begin{aligned}D_{a+\mathbf{1}} f &= D_a f + D_{\mathbf{1}} f + D_a D_{\mathbf{1}} f \\ &= D_a f + 1 + 0.\end{aligned}$$

Conversely, $D_{a+\mathbf{1}} f = D_a f + 1$ for $a = 0$ leads to $D_{\mathbf{1}} f = 1$. □

From simulation results, trivial balanced functions are expected to form a very large subset of all balanced symmetric functions. Actually, the exhaustive search for all balanced symmetric functions up to 128 variables presented in [8] show that, for odd $n$, all balanced symmetric functions are trivial balanced except for

$$n \in \{13, 29, 31, 33, 35, 41, 47, 61, 63, 73, 97, 103\}.$$

Similarly, balanced symmetric functions of an even number of variables $n \leq 128$ which are not affine only exist if $n = 6t+2$ for some $t$ or if $n \in \{24, 34, 48, 54\}$. Moreover, the nonexistence of nonaffine balanced symmetric functions has been proved in the following case.

*Proposition 6 [8, Theorem 2.1]:* Let $p$ be a prime and $f \in \mathcal{B}_{p-1}$ be a symmetric function. If $f$ is balanced, then $f$ has degree 1.

## IV. Resiliency of Symmetric Boolean Functions

In many cryptographic applications, it is required that the output of the involved Boolean function be not correlated to a small subset of its input variables. Otherwise, a statistical dependence between the output and a few inputs can be exploited in some attacks, such as correlation attacks [15]. For instance, the function used to combine several linear feedback shift registers in order to generate a pseudorandom sequence in a stream cipher must remain balanced if a few coordinates of the input vector are kept constant. This leads to the notion of resiliency.

*Definition 6:* [15] A balanced Boolean function of $n$ variables is $t$-resilient if it remains balanced when any $t$ input variables are fixed.

There is no general bound on the order of resiliency of symmetric Boolean functions. However, an infinite family of 2-resilient functions was exhibited in [7], while some infinite families of third-order correlation-immune functions were found in [9]. In [8], some infinite families of 1- and 2-resilient functions were found and a computer search up to $n = 128$ has lead to the conjecture that there does not exist any 3-resilient symmetric function of $n$ variables except the affine functions.

### A. Restrictions of a Symmetric Function

The notion of resiliency is obviously related to the weights of the restrictions of the function to some subspaces. For any $f \in \mathcal{B}_n$ and any affine subspace $V \subset \boldsymbol{F}_2^n$, the restriction of $f$ to $V$ is the function

$$\begin{aligned} f_V : V &\to \boldsymbol{F}_2 \\ x &\mapsto f(x). \end{aligned}$$

Then, $f_V$ can obviously be identified with a Boolean function of $\dim(V)$ variables.

Now, we focus on a subspace $V$ spanned by $k$ canonical basis vectors and its supplementary subspace $\overline{V}$. We consider the restrictions of $f$ to $V$ and to all its cosets $a + V$, $a \in \overline{V}$. It is worth noticing that, when $f$ is symmetric, we can choose $V = \langle e_1, \ldots, e_k \rangle$ without loss of generality. Moreover, if $f$ is symmetric, then $f_{a+V}$ is a symmetric Boolean function of $k$ variables. Indeed, for all $x \in V$

$$f_{a+V}(x) = f(a+x) = v_f(\mathrm{wt}(a) + \mathrm{wt}(x))$$

which only depends on the weight of $x$ when $a$ is fixed. Moreover, the simplified value vector and the simplified ANF vector of $f_{a+V}$ can be deduced from $f$ as follows.

*Proposition 7:* Let $f \in \mathcal{B}_n$ be a symmetric function and $V = \langle e_1, \ldots e_k \rangle$ where $k \leq n$. For any $a \in \overline{V} = \langle e_{k+1}, \ldots, e_n \rangle$, the restriction of $f$ to $a + V$ is a symmetric function of $k$ variables which only depends on $\mathrm{wt}(a)$. Its simplified value vector and its simplified ANF vector are given by: for any $i$, $0 \leq i \leq k$

$$\begin{aligned} v_{f_{a+V}}(i) &= v_f(i + \mathrm{wt}(a)) \\ \lambda_{f_{a+V}}(i) &= \bigoplus_{j \preceq \mathrm{wt}(a)} \lambda_f(i+j). \end{aligned}$$

*Proof:* Let

$$f(x) = \bigoplus_{u \in \boldsymbol{F}_2^n} \lambda_u \prod_{i=1}^{n} x_i^{u_i}, \qquad x \in \boldsymbol{F}_2^n$$

be the ANF of $f$. Then, we have, for any $x \in V$

$$\begin{aligned} f_{a+V}(x) &= \bigoplus_{u \in \boldsymbol{F}_2^k} \bigoplus_{v \in \boldsymbol{F}_2^{n-k}} \lambda_{u,v} \prod_{i=1}^{k} x_i^{u_i} \prod_{j=1}^{n-k} a_j^{v_j} \\ &= \bigoplus_{u \in \boldsymbol{F}_2^k} \prod_{i=1}^{k} x_i^{u_i} \bigoplus_{v \in \boldsymbol{F}_2^{n-k}} \lambda_{u,v} \prod_{j=1}^{n-k} a_j^{v_j}. \end{aligned}$$

Moreover,

$$\prod_{j=1}^{n-k} a_j^{v_j} = 1 \text{ if and only if } \mathrm{supp}(v) \subseteq \mathrm{supp}(a)$$

i.e., $v \preceq a$. Thus, we get

$$f_{a+V}(x) = \bigoplus_{u \in \boldsymbol{F}_2^k} \prod_{i=1}^{k} x_i^{u_i} \bigoplus_{v \preceq a} \lambda_{u,v}.$$

Since $f$ is symmetric, $\lambda_{u,v} = \lambda_f(\mathrm{wt}(u) + \mathrm{wt}(v))$. Therefore,

$$\begin{aligned} \bigoplus_{v \preceq a} \lambda_{u,v} &= \bigoplus_{j=0}^{\mathrm{wt}(a)} \binom{\mathrm{wt}(a)}{j} \lambda(\mathrm{wt}(u) + j) \\ &= \bigoplus_{j \preceq \mathrm{wt}(a)} \lambda_f(\mathrm{wt}(u) + j). \end{aligned}$$

We finally deduce the ANF of $f_{a+V}$

$$f_{a+V}(x) = \bigoplus_{i=0}^{k} \left( \bigoplus_{j \preceq \mathrm{wt}(a)} \lambda_f(j+i) \right) X_{i,k}. \qquad \square$$

As an immediate corollary, we deduce the following property on the degrees of the restrictions of a symmetric function, which does not hold in general for any Boolean function.

*Corollary 1:* Let $f \in \mathcal{B}_n$ be a symmetric function of degree $d$ and $V = \langle e_1, \ldots e_k \rangle$ where $d \leq k \leq n$. The restrictions of $f$ to all $a + V$, $a \in \overline{V} = \langle e_{k+1}, \ldots, e_n \rangle$, have degree $d$.

### B. Resiliency Order and Regular Patterns in the Simplified Value Vector

Now, we focus on the relationship between the existence of some regular patterns in the simplified value vector of a symmetric function and its order of resiliency.

*Proposition 8:* Let $f \in \mathcal{B}_n$ be a $t$-resilient symmetric function whose simplified value vector is ultimately periodic, i.e., $v_f(i) = v_f(i+T)$ for all $i \geq n_0$, with $n_0 + T - 1 \leq t$. Then, for any $m \geq 0$, there exists a symmetric Boolean function of $n+m$ variables with degree at least $\deg(f)$ which is $(t+m)$-resilient.

*Proof:* From Proposition 7, $f$ is $t$-resilient if and only if all $(n-t)$-variable symmetric functions with simplified value vectors

$$v(f_i) = (v_f(i), v_f(i+1), \ldots, v_f(n-t+i))$$

for $0 \leq i \leq t$ are balanced. Moreover, we know from Corollary 1 that all these functions have the same degree as $f$ since $n - t \geq \deg(f)$ by Siegenthaler's inequality [15]. Since $f$ is ultimately periodic with period $T$, we have

$$v(f_{i+T}) = v(f_i), \qquad \forall\, i \geq n_0.$$

Therefore, for all $k \geq t$, the functions with simplified value vectors

$$v(f_k) = v(f_{n_0 + (k - n_0) \bmod T})$$

are balanced because $n_0 \leq n_0 + (k - n_0) \bmod T \leq t$. Then, for any $m \geq 0$, we consider the $(n+m)$-variable function

$g_m$ whose simplified value vector consists of the first $(n+m)$ elements of $(v_0 \dots v_{n_0-1}(v_{n_0} \dots v_{n_0+T-1})^*)$. All restrictions of $g_m$ to the cosets of $\langle e_1, \dots, e_{n-t} \rangle$ are balanced, which means that $g_m$ is $(t+m)$-resilient. Moreover, their degrees are equal to $\deg(f)$, implying that $\deg(g_m) \geq \deg(f)$. □

In the previous proposition, one has to be especially sensitive to the condition $n_0 + T \leq t+1$. It means that among the $(t+1)$ balanced symmetric functions of $(n-t)$ variables obtained by restricting the $t$-resilient function $f$, some functions are equal, due to the periodicity property.

*Corollary 2:* Let $f \in \mathcal{B}_n$ be a symmetric function whose simplified value vector is ultimately periodic, i.e., $v_f(i) = v_f(i+T)$ for all $i \geq n_0$. If $f$ is $t$-resilient with $t \geq n_0 + T - 1$, then $\deg(f) = 1$.

*Proof:* Let $p$ be any prime number such that $p > n$. From the previous proposition, there exists a function $g$ of $(p-1)$ variables with $\deg(g) \geq \deg(f)$ which is balanced (because of its resiliency order). Proposition 6 then implies that $\deg(g) = 1 \geq \deg(f)$. □

The previous result can be first applied to the symmetric functions with periodic simplified value vectors. It points out that the order of resiliency of a symmetric function is limited by its degree.

*Theorem 2:* Let $f \in \mathcal{B}_n$ be a symmetric function with $\deg(f) \leq 2^\ell$. If $f$ is $(2^\ell - 1)$-resilient, then $\deg(f) = 1$.

*Proof:* If $\deg(f) \leq 2^\ell - 1$, $v(f)$ is periodic with period $2^\ell$ (Theorem 1). Then, the result can be immediately deduced from the previous corollary. If $deg(f) = 2^\ell$, we know from Proposition 4 that $v(f)$ is a part of $(v_0, \dots, v_{2^\ell-1}, v_0 \oplus 1, \dots, v_{2^\ell-1} \oplus 1)$, for some $v_0, \dots, v_{2^\ell-1} \in \boldsymbol{F}_2$. $f$ is $(2^\ell - 1)$-resilient if and only if all symmetric functions with simplified value vectors

$$v(f_i) = \big(v_f(i), v_f(i+1), \dots, v_f(n-2^\ell+1+i)\big)$$

for $0 \leq i < 2^\ell$ are balanced. The functions obtained by complementing these vectors, i.e.,

$$v(f_{i+2^\ell}) = \big(v_f(i) \oplus 1, v_f(i+1) \oplus 1, \dots, v_f(n-2^\ell+1+i) \oplus 1\big)$$

are obviously balanced for any $0 \leq i < 2^\ell$. By the same argument as in Proposition 8, we deduce that for any $m \geq 0$, the $(n+m)$-variable function whose simplified value vector consists of the first $(n+m)$ elements of $(v_0, \dots, v_{2^\ell-1}, v_0 \oplus 1, \dots, v_{2^\ell-1} \oplus 1)^*$ is $(2^\ell - 1 + m)$-resilient and its degree is at least $\deg(f)$. For $m = p - n - 1$ where $p$ is any prime number with $p > n$, we get that $\deg(f) = 1$. □

Proposition 8 also enables to prove that all restrictions of resilient functions are distinct. More precisely, we have the following.

*Proposition 9:* If there exists a symmetric $t$-resilient function of $n$ variables with degree $d \neq 1$, then there exist $(t+1)$ distinct balanced symmetric functions of $(n-t)$ variables with degree $d$.

*Proof:* We have to prove that the $(t+1)$ symmetric functions $f_i$ of $(n-t)$ variables, defined by their simplified value vectors

$$v(f_i) = (v_f(i), v_f(i+1), \dots, v_f(n-t+i)), \qquad 0 \leq i \leq t$$

are distinct. Suppose that $f_j = f_k$ for some $(j,k)$ with $0 \leq j < k \leq t$. Then, the simplified value vectors $v(f_{j+1})$ and $v(f_{k+1})$ are either equal or they differ on their last component, i.e.,

$$v(f_{j+1}) \oplus v(f_{k+1}) = (0, 0 \dots, 0, 1).$$

In this second case, $f_{j+1} + f_{k+1}$ has degree $(n-t)$ since its Hamming weight is odd. But, $\deg(f) \leq n - t$ because $f$ is $t$-resilient, implying that $\deg(f_{j+1}) = \deg(f_{k+1}) = \deg(f)$ (from Corollary 1), a contradiction. Therefore, $f_{j+1} = f_{k+1}$, and we deduce by induction that $f_{j+m} = f_{k+m}$ for all $m \leq t-k$. It means that the simplified value vector of $f$ is ultimately periodic: for all $i$ such that $j \leq i \leq t - k + j$

$$v_f(i+k-j) = v_f(i).$$

It follows from Corollary 2 that $f$ has degree 1. □

Now, we focus on 1-resilient symmetric functions. A straightforward method for constructing 1-resilient symmetric functions of an even number of variables might be to start from trivial balanced restrictions. However, we can prove that this construction always leads to affine functions.

*Proposition 10:* Let $n$ be an even integer and let $f \in \mathcal{B}_n$ be a symmetric function. Let $H = \langle e_1, \dots e_{n-1} \rangle$. If both restrictions of $f$ to $H$ and $e_n + H$ are trivial balanced functions, then $\deg(f) = 1$.

*Proof:* Assume that $f_H$ and $f_{e_n+H}$ are trivial balanced functions. It means for $f_H$ that $\forall\, i, 0 \leq i \leq n-1$, $v_f(i) = v_f(n-1-i) \oplus 1$, and for $f_{e_n+H}$ that $\forall\, j, 1 \leq j \leq n$, $v_f(j) = v_f(n-j+1) \oplus 1$. Then, we get the system

$$\begin{aligned} v_f(i) &= v_f(n-1-i) \oplus 1, \quad \forall\, i,\ 0 \leq i \leq n-1 \\ v_f(n-1-i) &= v_f(i+2) \oplus 1, \quad \forall\, i,\ 0 \leq i \leq n-2. \end{aligned}$$

Thus, for all $i$, $0 \leq i \leq n-2$, $v_f(i) = v_f(i+2)$. Theorem 1 implies that $\deg(f) \leq 1$. Since $f$ cannot be constant because its restrictions are balanced, it has degree 1. □

A careful examination of the list of all 2-resilient symmetric functions up to 128 variables [8] shows that all 2-resilient functions are trivial balanced. From the previous proposition, it implies that 3-resilient nonaffine symmetric functions up 128 variables do not exist. However, it is an open problem to determine whether this property holds for any number of variables.

## V. Derivatives of Symmetric Functions

In this section, we focus on the propagation characteristics of symmetric functions. They are determined by the cryptographic properties of their derivatives.

### A. General Properties of the Derivatives

First, we point out that all derivatives $D_a f$ of a symmetric function are linearly equivalent when $a$ has a fixed Hamming weight.

*Proposition 11:* Let $f \in \mathcal{B}_n$ be a symmetric function and let $a, b \in \boldsymbol{F}_2^n$ be such that $\mathrm{wt}(a) = \mathrm{wt}(b)$. Then, $D_a f$ and $D_b f$ are linearly equivalent, i.e., there exists a linear permutation $\sigma$ of $\boldsymbol{F}_2^n$ such that $D_a f = D_b f \circ \sigma$.

*Proof:* Let $a,b \in \boldsymbol{F}_2^n$ such that $\mathrm{wt}(a) = \mathrm{wt}(b)$. There exists a permutation $\sigma$ on $\{1,\dots,n\}$ such that $b = \sigma(a)$. Then, $\sigma$ is a linear permutation of $\boldsymbol{F}_2^n$. Since $f$ is symmetric, we have

$$\begin{aligned} D_b f(\sigma(x)) &= f(\sigma(x)) \oplus f(\sigma(x)+b) \\ &= f(x) \oplus f(\sigma(x)+\sigma(a)) \\ &= f(x) \oplus f(\sigma(x+a)) \\ &= f(x) \oplus f(x+a) \\ &= D_a f(x). \end{aligned}$$ □

Since most properties of the derivatives we consider, especially the weight and the degree, are invariant under composition by a linear transformation, we only study the derivatives of a symmetric function with respect to the vectors $\varepsilon_k = e_{n-k+1} + \cdots + e_n$ of weight $k$ for $1 \le k \le n$.

The derivatives of a symmetric function are not symmetric in general. However, they can be decomposed into symmetric functions.

*Proposition 12:* Let $f \in \mathcal{B}_n$ be a symmetric function. Let $k$ be an integer, $1 \le k \le n-1$, $V = \langle e_1,\dots,e_{n-k}\rangle$, and $\varepsilon_k = e_{n-k+1} + \cdots + e_n$. Then, the restrictions of $D_{\varepsilon_k} f$ to all affine subspaces $b+V$, $b \in \langle e_{n-k+1},\dots,e_n\rangle$

$$\begin{aligned} g_b : V &\to \boldsymbol{F}_2 \\ x &\mapsto D_{\varepsilon_k} f(x+b) \end{aligned}$$

are symmetric functions of $(n-k)$ variables and they only depend on $\mathrm{wt}(b)$. Moreover, their simplified value vectors and ANF vectors are given for all $0 \le i \le n-k$ by

$$\begin{aligned} v_{g_b}(i) &= v_f(i+\mathrm{wt}(b)) \oplus v_f(i+k-\mathrm{wt}(b)) \\ \lambda_{g_b}(i) &= \bigoplus_{j \preceq k-\mathrm{wt}(b)} \lambda_f(i+j) \oplus \bigoplus_{j \preceq \mathrm{wt}(b)} \lambda_f(i+j). \end{aligned}$$

*Proof:* Let $b \in \overline{V} = \langle e_{n-k+1},\dots,e_n\rangle$. Then, for any $y = x+b$ with $x \in V$, we have

$$\begin{aligned} \mathrm{wt}(y) &= \mathrm{wt}(x) + \mathrm{wt}(b) \\ \mathrm{wt}(y+\varepsilon_k) &= \mathrm{wt}(x) + \mathrm{wt}(b+\varepsilon_k) \\ &= \mathrm{wt}(x) + k - \mathrm{wt}(b). \end{aligned}$$

Thus, for any $x \in V$

$$\begin{aligned} D_{\varepsilon_k} f(x+b) &= f(x+b) \oplus f(x+\varepsilon_k+b) \\ &= v_f(\mathrm{wt}(x)+\mathrm{wt}(b)) \oplus v_f(\mathrm{wt}(x)+k-\mathrm{wt}(b)) \end{aligned}$$

which shows that $g_b$ is symmetric and only depends on $\mathrm{wt}(b)$.

Now, we compute the simplified ANF vector of $g_b$. Let us decompose the algebraic normal formal of $f$ as

$$f(x+y) = \bigoplus_{u \in \boldsymbol{F}_2^{n-k}} \bigoplus_{v \in \boldsymbol{F}_2^k} \lambda_{u,v} \prod_{i=1}^{n-k} x_i^{u_i} \prod_{j=n-k+1}^{n} y_j^{v_j}.$$

for $(x,y) \in (V,\overline{V})$.

Then, for any $b \in \overline{V}$ and $x \in V$, we have

$$\begin{aligned} g_b(x) &= D_{\varepsilon_k} f(x+b) \\ &= \bigoplus_{u \in \boldsymbol{F}_2^{n-k}} \bigoplus_{v \in \boldsymbol{F}_2^k} \lambda_{u,v} \prod_{i=1}^{n-k} x_i^{u_i} \\ &\quad \times \left( \prod_{i=1}^{k} (b_i \oplus 1)^{v_i} \oplus \prod_{i=1}^{k} b_i^{v_i} \right). \end{aligned}$$

But, $\prod_{i=1}^{k} b_i^{v_i} = 1$ if and only if $\mathrm{supp}(v) \subseteq \mathrm{supp}(b)$, i.e., $v \preceq b$. We then get

$$g_b(x) = \bigoplus_{u \in \boldsymbol{F}_2^{n-k}} \prod_{i=1}^{n-k} x_i^{u_i} \left( \bigoplus_{v \preceq \bar{b}} \lambda_{u,v} \oplus \bigoplus_{v \preceq b} \lambda_{u,v} \right)$$

where $\bar{b} = b + \varepsilon_k$. Since $f$ is symmetric, we have $\lambda_{u,v} = \lambda_f(\mathrm{wt}(u)+\mathrm{wt}(v))$. Therefore,

$$\begin{aligned} &\bigoplus_{v \preceq \bar{b}} \lambda_{u,v} \oplus \bigoplus_{v \preceq b} \lambda_{u,v} \\ &\quad = \left( \bigoplus_{i=0}^{k-\mathrm{wt}(b)} \lambda_f(\mathrm{wt}(u)+i) \binom{k-\mathrm{wt}(b)}{i} \right) \\ &\qquad \oplus \left( \bigoplus_{i=0}^{\mathrm{wt}(b)} \lambda_f(\mathrm{wt}(u)+i) \binom{\mathrm{wt}(b)}{i} \right) \\ &\quad = \bigoplus_{i \preceq k-\mathrm{wt}(b)} \lambda_f(\mathrm{wt}(u)+i) \oplus \bigoplus_{i \preceq \mathrm{wt}(b)} \lambda_f(\mathrm{wt}(u)+i). \end{aligned}$$

Thus, the coefficients of the algebraic normal form of the $(n-k)$-variable function $g_b$ are given by: for any $0 \le j \le n-k$

$$\lambda_{g_b}(j) = \bigoplus_{i \preceq k-\mathrm{wt}(b)} \lambda_f(j+i) \oplus \bigoplus_{i \preceq \mathrm{wt}(b)} \lambda_f(j+i).$$ □

We can illustrate the previous result by applying it to the derivatives of a symmetric function with respect to a vector of weight 1 or 2.

*Corollary 3:* Let $f \in \mathcal{B}_n$ be a symmetric function. Then, the algebraic normal forms of $D_{e_n} f$ and of $D_{e_{n-1}+e_n} f$ are

$$\begin{aligned} D_{e_n} f(x) &= \bigoplus_{i=0}^{n-1} \lambda_f(i+1) X_{i,n-1} \\ D_{e_{n-1}+e_n} f(x) &= (x_{n-1} \oplus x_n \oplus 1) \bigoplus_{i=0}^{n-2} \lambda_f(i+2) X_{i,n-2}. \end{aligned}$$

*Proof:* For $k=1$, we know from the previous proposition that the restrictions of $D_{e_n} f$ to $H = \langle e_1,\dots,e_{n-1}\rangle$ and to $e_n + H$, denoted by $g_0$ and $g_1$ are equal. For any $0 \le i \le n-1$, their simplified ANF vector is given by

$$\begin{aligned} \lambda_{g_0}(i) &= \lambda_{g_1}(i) \\ &= \bigoplus_{j \preceq 1} \lambda_f(i+j) \oplus \bigoplus_{j \preceq 0} \lambda_f(i+j) \\ &= \lambda_f(i+1). \end{aligned}$$

Thus,

$$\begin{aligned} D_{e_n}f(x) &= (x_n \oplus 1)g_0(x_1,\ldots,x_{n-1}) \oplus x_n g_1(x_1,\ldots,x_{n-1}) \\ &= g_0(x_1,\ldots,x_{n-1}) \\ &= \bigoplus_{i=0}^{n-1} \lambda_f(i+1)X_{i,n-1}. \end{aligned}$$

For $k=2$ and $V=\langle e_1,\ldots,e_{n-2}\rangle$, we denote by $g_0$, $g_1$, and $g_2$ the restrictions of $D_{e_{n-1}+e_n}f$ to $V$, to $e_n+V$ (or equivalently, to $e_{n-1}+V$) and to $e_{n-1}+e_n+V$. We deduce from the previous proposition that, for any $i$, $0 \le i \le n-2$

$$\begin{aligned} \lambda_{g_0}(i) &= \lambda_{g_2}(i) \\ &= \bigoplus_{j\preceq 2} \lambda_f(i+j) \oplus \bigoplus_{j\preceq 0} \lambda_f(i+j) \\ &= \lambda_f(i+2) \end{aligned}$$

and

$$\lambda_{g_1}(i) = \bigoplus_{j\preceq 1} \lambda_f(i+j) \oplus \bigoplus_{j\preceq 1} \lambda_f(i+j) = 0.$$

Then

$$D_{e_{n-1}+e_n}f(x) = (x_{n-1} \oplus x_n \oplus 1) \bigoplus_{i=0}^{n-2} \lambda_f(i+2)X_{i,n-2}. \quad \square$$

The previous formula points out that

$$\deg(D_{e_{n-1}+e_n}f) = \deg(f) - 1.$$

We can then deduce the following corollary. It generalizes a result due to Dawson and Wu [14] which shows that the only possible linear structure for a nonaffine symmetric function is the all-one vector. Further necessary conditions on the existence of linear structure will be determined in Section V-C.

*Corollary 4:* Let $f \in \mathcal{B}_n$ be a symmetric function. Then, for all $a \in \boldsymbol{F}_2^n \setminus \{0, \mathbf{1}\}$, $\deg(D_a f) = \deg(f) - 1$.

*Proof:* For any $a \in \boldsymbol{F}_2^n$ such that $a \neq 0$, $\mathbf{1}$, there exists $b \in \boldsymbol{F}_2^n$ such that $\mathrm{wt}(b) = \mathrm{wt}(a)$ and $\mathrm{wt}(a+b) = 2$. Then, we have

$$D_a f + D_b f = D_{a+b} f + D_a D_b f.$$

Clearly, both $D_a f$ and $D_b f$ have degree at most $\deg(f) - 1$, and $\deg(D_a D_b f) \le \deg(f) - 2$. Moreover, we know from the previous corollary that $D_{a+b}f$ has degree exactly $\deg(f) - 1$ since $\mathrm{wt}(a+b)=2$. Therefore, $D_a f + D_b f$ has degree $\deg(f)-1$, implying that $\deg(D_a f)=\deg(f)-1$. $\square$

### B. Symmetric Functions Satisfying the Propagation Criterion

Some cryptographic applications require that the output difference of the involved Boolean function be uniformly distributed for low-weight input differences. This property, referred as propagation criterion [16], is notably important when the function is used in a hash function or in a block cipher.

*Definition 7 [16]:* A function $f \in \mathcal{B}_n$ satisfies the propagation criterion of degree $k$ ($PC(k)$) if $\mathcal{F}(D_a f) = 0$ for all $a \in \boldsymbol{F}_2^n$ such that $1 \le \mathrm{wt}(a) \le k$.

It is well known that the $n$-variable functions satisfying $PC(n)$ are the bent functions [17]. The symmetric functions satisfying $PC(n)$ are the quadratic functions of an even number of variables [5]. Here, we obtain a similar characterization of the symmetric functions satisfying $PC(2)$. Proposition 12 and Corollary 3 lead to the following theorem, which has been independently proved by Gouget [18].

*Theorem 3:* The symmetric Boolean functions of $n$ variables satisfying the propagation criterion of order 2 are the quadratic functions. Moreover, they satisfy $PC(n)$ if $n$ is even and $PC(n-1)$ if $n$ is odd.

*Proof:* Let $V=\langle e_1,\ldots,e_{n-2}\rangle$. We denote by $g_0$, $g_1$, and $g_2$ the restrictions of $D_{e_{n-1}+e_n}f$ to $V$, to $e_n+V$ (or equivalentl,y to $e_{n-1}+V$) and to $e_{n-1}+e_n+V$. The weight of $D_{e_{n-1}+e_n}f$ is

$$\mathrm{wt}(D_{e_{n-1}+e_n}f) = \mathrm{wt}(g_0) + 2\mathrm{wt}(g_1) + \mathrm{wt}(g_2).$$

But, we know from Corollary 3 that $g_0 = g_2$ and $g_1 = 0$. As a consequence, $D_{e_{n-1}+e_n}f$ is balanced if and only if $g_0 = g_2 = 1$. Proposition 12 gives the simplified ANF vector of $g_0$ and $g_2$

$$\lambda_{g_0}(i) = \lambda_{g_2}(i) = \lambda_f(i+2)$$

implying that $g_0$ is the constant function equal to 1 if and only if $\lambda_f(2) = 1$ and $\forall\, i,\ i \ge 3$, $\lambda_f(i) = 0$, i.e., $\deg(f) = 2$.

Moreover, all derivatives of a quadratic symmetric function with respect to $a \in \boldsymbol{F}_2^n \setminus \{0, \mathbf{1}\}$ are balanced because they have degree 1 (Corollary 4). Therefore, the quadratic functions are exactly those satisfying $PC(n-1)$. Additionally, when $n$ is even, we also have that $D_{\mathbf{1}}f$ is balanced [5], implying that the function satisfies $PC(n)$. $\square$

Therefore, the only open problem is the characterization of the symmetric functions satisfying $PC(1)$. A large subset of these functions are those whose derivatives with respect to any vector of weight 1 have trivial balanced restrictions (in the sense of Proposition 12). These functions can be characterized as follows.

*Proposition 13:* Let $f \in \mathcal{B}_n$, $n$ even, be a symmetric function. Then, the following assertions are equivalent:

i) $f$ satisfies $PC(1)$ and the restriction of $D_{e_n}f$ to $\langle e_1,\ldots,e_{n-1}\rangle$ is a trivial balanced function;
ii) $D_{\mathbf{1}}f = \varphi_{\mathbf{1}} + \varepsilon$, $\varepsilon \in \boldsymbol{F}_2$;
iii) $\forall\, a \in \boldsymbol{F}_2^n$, $\mathcal{F}(f+\varphi_a) = (-1)^{\mathrm{wt}(a)+\varepsilon}\mathcal{F}(f+\varphi_{\overline{a}})$.

Moreover, if $f$ verifies one of the properties above, then $D_a f$ is balanced for all $a \in \boldsymbol{F}_2^n$ with odd Hamming weight.

*Proof:* First we show that i) and ii) are equivalent. In the following, $g$ denotes the $(n-1)$-variable symmetric function corresponding to the restriction of $D_{e_n}f$ to $\langle e_1,\ldots,e_{n-1}\rangle$ (or equivalently, to $e_n + \langle e_1,\ldots,e_{n-1}\rangle$). From Proposition 7, we have

$$v_g(i) = v_f(i) \oplus v_f(i+1), \qquad \forall\, i,\ 0 \le i \le n-1.$$

Therefore, $g$ is a trivial balanced function if and only if, for all $0 \le i \le n-1$, $v_g(i) = v_g(n-1-i) \oplus 1$, which means that for all $i$, $0 \le i \le n-1$

$$v_f(i) \oplus v_f(i+1) = v_f(n-i-1) \oplus v_f(n-i) \oplus 1. \quad (1)$$

Clearly, $D_{\mathbf{1}}f$ is a symmetric function of $n$ variables since it satisfies

$$D_{\mathbf{1}}f(x) = f(x) \oplus f(x+\mathbf{1}) = v_f(\mathrm{wt}(x)) \oplus v_f(n - \mathrm{wt}(x)).$$

Then, (1) is equivalent to

$$v_{D_1}(i) = v_{D_1}(i+1) \oplus 1, \qquad \forall\, i,\ 0 \le i \le n-1$$

which means that $D_{\mathbf{1}}f$ has degree 1 (Theorem 1).

Now, we prove that ii) and iii) are equivalent. To that purpose, we calculate $\mathcal{F}(f + D_{\mathbf{1}}f + \varphi_a)$, $a \in \boldsymbol{F}_2^n$

$$\begin{aligned}\mathcal{F}(f + D_{\mathbf{1}}f + \varphi_a) &= \sum_{x \in \boldsymbol{F}_2^n} (-1)^{f(x+\mathbf{1}) \oplus a \cdot x} \\ &= (-1)^{\mathrm{wt}(a)} \sum_{x \in \boldsymbol{F}_2^n} (-1)^{f(x) \oplus a \cdot x} \\ &= (-1)^{\mathrm{wt}(a)} \mathcal{F}(f + \varphi_a).\end{aligned}$$

However, $D_{\mathbf{1}}f = \varphi_{\mathbf{1}} + \varepsilon, \varepsilon \in \boldsymbol{F}_2$, if and only if for any $a \in \boldsymbol{F}_2^n$

$$\mathcal{F}(f + D_{\mathbf{1}}f + \varphi_a) = \mathcal{F}(f + \varphi_{\overline{a}} + \varepsilon) = (-1)^{\varepsilon} \mathcal{F}(f + \varphi_{\overline{a}}).$$

Therefore, $D_{\mathbf{1}}f = \varphi_{\mathbf{1}} + \varepsilon$ if and only if

$$\mathcal{F}(f + \varphi_{\overline{a}}) = (-1)^{\mathrm{wt}(a) + \varepsilon} \mathcal{F}(f + \varphi_a)$$

for all $a \in \boldsymbol{F}_2^n$.

Finally, we prove that iii) implies that $\forall\, a \in \boldsymbol{F}_2^n$, $\mathrm{wt}(a)$ odd, $\mathcal{F}(D_a f) = 0$. Let $H$ denote the hyperplane composed of all $n$-bit words with an even weight. We deduce from [10, Theorem V.1] that

$$\mathcal{F}^2(f + \varphi_a) + \mathcal{F}^2(f + \varphi_{\overline{a}}) = 2 \sum_{e \in H} (-1)^{a \cdot e} \mathcal{F}(D_e f).$$

On the other hand, assertion iii) implies that

$$\mathcal{F}^2(f + \varphi_a) + \mathcal{F}^2(f + \varphi_{\overline{a}}) = 2\mathcal{F}^2(f + \varphi_a).$$

But, we have

$$\mathcal{F}^2(f + \varphi_a) = \sum_{e \in \boldsymbol{F}_2^n} (-1)^{a \cdot e} \mathcal{F}(D_e f).$$

Thus, combining both equalities leads to

$$\sum_{e \in \overline{H}} (-1)^{a \cdot e} \mathcal{F}(D_e f) = 0$$

where $\overline{H} = \boldsymbol{F}_2^n \setminus H$. We deduce that for any $u \in \overline{H}$

$$\begin{aligned}&\sum_{a \in \boldsymbol{F}_2^n} (-1)^{a \cdot u} \sum_{e \in \overline{H}} (-1)^{a \cdot e} \mathcal{F}(D_e f) \\ &\quad = \sum_{e \in \overline{H}} \mathcal{F}(D_e f) \sum_{a \in \boldsymbol{F}_2^n} (-1)^{a \cdot (u+e)} \\ &\quad = 2^n \mathcal{F}(D_u f) = 0.\end{aligned}$$

□

### C. Derivative With Respect to the All-One Vector

Finally, we focus on the derivative of a symmetric function with respect to the all-one vector, since this is the only case which is not covered by Proposition 12. This case is of interest especially because it completely determines whether a symmetric function has a linear structure. Here, we express the algebraic normal form of $D_{\mathbf{1}}f$ as a function of the simplified ANF vector of $f$. We need the following lemma which involves the higher order derivatives of $f$: for any $k$-dimensional subspace $V \subset \boldsymbol{F}_2^n$, we denote by $D_V^{(k)} f$ the $k$th order derivative of $f \in \mathcal{B}_n$ with respect to $V$, i.e., the $n$-variable function

$$D_V^{(k)} f = D_{a_1} D_{a_2} \dots D_{a_k} f$$

where $(a_1, \dots, a_k)$ is any basis of $V$.

*Lemma 1:* The derivative of $f \in \mathcal{B}_n$ with respect to the all-one vector is

$$D_{\mathbf{1}}f = \sum_{k=1}^{n} \sum_{i=1}^{\binom{n}{k}} D_{V_{I_i}}^{(k)} f.$$

where $V_{I_i} = \langle e_{i_1}, \dots, e_{i_k} \rangle$ with $1 \le i_1 < \cdots < i_k \le n$.

*Proof:* The equality obviously holds for $n = 1$. Now, we prove it by induction on $n$. Let us write $f$ as

$$f(x_1, \dots, x_n) = x_n f_1(x_1, \dots, x_{n-1}) \oplus f_2(x_1, \dots, x_{n-1})$$

where $f_1, f_2 \in \mathcal{B}_{n-1}$. Then we have

$$\begin{aligned}&D_{\mathbf{1_n}} f(x_1, \dots, x_n) \\ &\quad = x_n f_1(x_1, \dots, x_{n-1}) \oplus f_2(x_1, \dots, x_{n-1}) \\ &\qquad \oplus (x_n \oplus 1) f_1(x_1 \oplus 1, \dots, x_{n-1} \oplus 1) \\ &\qquad \oplus f_2(x_1 \oplus 1, \dots, x_{n-1} \oplus 1) \\ &\quad = x_n D_{\mathbf{1_{n-1}}} f_1(x_1, \dots, x_{n-1}) \oplus D_{\mathbf{1_{n-1}}} f_2(x_1, \dots, x_{n-1}) \\ &\qquad \oplus f_1(x_1 \oplus 1, \dots, x_{n-1} \oplus 1).\end{aligned}$$

On the other hand, we evaluate the expression

$$A_n(f) = \sum_{k=1}^{n} \sum_{i=1}^{\binom{n}{k}} D_{V_{I_i}}^{(k)} f$$

where $V_{I_i} = \langle e_{i_1}, \dots, e_{i_k} \rangle$, $1 \le i_1 < \cdots < i_k \le n$.

$$\begin{aligned}A_n(f) &= \sum_{k=1}^{n} \sum_{i=1}^{\binom{n}{k}} D_{V_{I_i}}^{(k)} (x_n f_1 + f_2) \\ &= \sum_{k=1}^{n-1} \sum_{i=1}^{\binom{n-1}{k}} D_{V_{I_i}}^{(k)} (x_n f_1 + f_2) \\ &\quad + \sum_{k=1}^{n-1} \sum_{i=1}^{\binom{n-1}{k}} D_{e_n} D_{V_{I_i}}^{(k)} (x_n f_1 + f_2) \\ &\quad + D_{e_n} (x_n f_1 + f_2) \\ &= x_n A_{n-1}(f_1) + A_{n-1}(f_2) + A_{n-1}(f_1) + f_1.\end{aligned}$$

By applying the induction hypothesis to $f_1$ and $f_2$, we deduce $A_n(f) = x_n D_{\mathbf{1_{n-1}}} f_1 + D_{\mathbf{1_{n-1}}} f_2 + D_{\mathbf{1_{n-1}}} f_1 + f_1 = D_{\mathbf{1_n}} f$. □

Thus, we deduce the algebraic normal form of $D_{\mathbf{1}}f$.

*Proposition 14:* Let $f \in \mathcal{B}_n$ be a symmetric function. Its derivative with respect to the all-one vector is a symmetric Boolean function of $n$ variables whose simplified value vector and ANF vector are given by

$$\begin{aligned}v_{D_{\mathbf{1}}f}(i) &= v_f(i) \oplus v_f(n-i) \\ \lambda_{D_{\mathbf{1}}f}(i) &= \bigoplus_{\substack{k \preceq n-i \\ k \ne 0}} \lambda_f(i+k)\end{aligned}$$

for all $i$, $0 \le i \le n$.

*Proof:* The relation between the simplified value vectors of $f$ and $D_{\mathbf{1}}f$ directly follows from the definition. We now de-

termine the simplified ANF vector of $D_{\mathbf{1}}f$. From the previous lemma, we have

$$D_{\mathbf{1}}f = \sum_{k=1}^{n} \sum_{i=1}^{\binom{n}{k}} D^{(k)}_{V_{I_i}} f$$

where $V_{I_i} = \langle e_{i_1}, \ldots, e_{i_k} \rangle$, $1 \le i_1 < \cdots < i_k \le n$.

The $k$th order derivative $D^{(k)}_{V_{I_i}} f$ only depends on the $(n-k)$ variables whose indices belong to

$$\{1, \ldots, n\} - \{i_1, \ldots, i_k\} = \overline{\{i_1, \ldots, i_k\}}.$$

More precisely, we deduce from Corollary 3 that

$$D^{(k)}_{V_{I_i}} f = \bigoplus_{i=0}^{n-k} \lambda_f(i+k) X_{i, \overline{\{i_1, \ldots, i_k\}}}.$$

Therefore,

$$\left( \sum_{i=1}^{\binom{n}{k}} D^{(k)}_{V_{I_i}} f \right)(x) = \bigoplus_{1 \le i_1 < \cdots < i_k \le n} \bigoplus_{i=0}^{n-k} \lambda_f(i+k) X_{i, \overline{\{i_1, \ldots, i_k\}}} = \bigoplus_{i=0}^{n-k} \lambda_f(i+k) \bigoplus_{1 \le i_1 < \cdots < i_k \le n} X_{i, \overline{\{i_1, \ldots, i_k\}}}.$$

We now have to simplify the sum

$$\bigoplus_{1 \le i_1 < \cdots < i_k \le n} X_{i, \overline{\{i_1, \ldots, i_k\}}}.$$

It is composed of $\binom{n}{n-k}$ elementary symmetric polynomials of degree $i$, but which may have some variables in common. For any fixed subset of $i$ indices, the product of the $i$ corresponding variables appears in exactly $\binom{n-i}{n-k-i}$ terms $X_{i,\{\ldots\}}$. Therefore, the sum consists of all products of $i$ variables, each of them being repeated $\binom{n-i}{n-k-i}$ times, i.e.,

$$\bigoplus_{1 \le i_1 < \cdots < i_k \le n} X_{i, \overline{\{i_1, \ldots, i_k\}}} = \binom{n-i}{n-k-i} X_{i,n}.$$

Then, we have

$$\left( \sum_{i=1}^{\binom{n}{k}} D^{(k)}_{V_{I_i}} f \right)(x) = \bigoplus_{i=0}^{n-k} \lambda_f(i+k) \left( \binom{n-i}{n-k-i} \bmod 2 \right) X_{i,n}.$$

We finally get

$$\begin{aligned} D_{\mathbf{1}}f(x) &= \bigoplus_{k=1}^{n} \left( \bigoplus_{i=0}^{n-k} \lambda_f(i+k) \left( \binom{n-i}{k} \bmod 2 \right) X_{i,n} \right) \\ &= \bigoplus_{i=0}^{n-1} \left( \bigoplus_{k=1}^{n-i} \lambda_f(i+k) \left( \binom{n-i}{k} \bmod 2 \right) \right) X_{i,n} \\ &= \bigoplus_{i=0}^{n-1} \bigoplus_{\substack{k \preceq n-i \\ k \neq 0}} \lambda_f(i+k) X_{i,n}. \end{aligned}$$

□

We immediately deduce the following result on the degree of $D_{\mathbf{1}}f$.

*Proposition 15:* Let $f \in \mathcal{B}_n$ be a symmetric function of degree $d$. Then $\deg(D_{\mathbf{1}}f) = d-1$ if and only if $(n-d)$ is even. Moreover, if $(n-d)$ is odd, we have $\deg(D_{\mathbf{1}}f) = d-2$ if $\lambda_f(d-1) = \frac{n-d-1}{2} \bmod 2$ and $\deg(D_{\mathbf{1}}f) \le \deg(f) - 4$ otherwise.

*Proof:* Let $\mu$ denote the simplified ANF vector of $D_{\mathbf{1}}f$. The coefficients are

$$\mu(i) = \bigoplus_{\substack{k \preceq n-i \\ k \neq 0}} \lambda_f(i+k).$$

We have

$$\mu(d-1) = \bigoplus_{\substack{k \preceq n-d+1 \\ k \neq 0}} \lambda_f(d-1+k)$$

which equals 0 if $1 \not\preceq n-d+1$, which means that $n-d$ is odd, and equals $\lambda_f(d)$ if and only if $1 \preceq n-d+1$ which means that $n-d$ is even. We need to calculate $\mu(d-2)$ in the case where $n-d$ is odd, getting

$$\mu(d-2) = \bigoplus_{\substack{k \preceq n-d+2 \\ k \neq 0}} \lambda_f(d-2+k).$$

A similar argument leads to the following:

- if $n-d \equiv 1 \bmod 4$ then $\mu(d-2) = \lambda_f(d) + \lambda_f(d-1)$ and $\mu(d-3) = 0$. Then
$$\deg(D_{\mathbf{1}}f) \begin{cases} = d-2, & \text{if } \lambda_f(d-1) = 0 \\ \le d-4, & \text{if } \lambda_f(d-1) = 1; \end{cases}$$
- if $n-d \equiv 3 \bmod 4$ then $\mu(d-2) = \lambda_f(d-1)$ and $\mu(d-3) = \lambda_f(d-1)$. Then
$$\deg(D_{\mathbf{1}}f) \begin{cases} = d-2, & \text{if } \lambda_f(d-1) = 1 \\ \le d-4, & \text{if } \lambda_f(d-1) = 0. \end{cases}$$

□

As an immediate corollary, we deduce that a symmetric function $f \in \mathcal{B}_n$, $\deg(f) \neq 1$, does not have any linear structure if $n - \deg(f)$ is even.

## VI. Symmetric Functions of Low Degree

It was established in Section III that the symmetric functions of low degree are characterized by simplified value vectors with a small period. This property, combined with the previous tools, enables us to provide an extended study of symmetric functions of degree less than 8. Most notably, we compute the Hamming weights of all these functions for any number of variables, and we exhibit all balanced symmetric functions of degree less than 8. We also characterize, in terms of Walsh spectrum and propagation characteristics, all symmetric functions of degree 2 and 3 since their simplified value vectors have period 4.

Thanks to the periodicity of its simplified value vector, we can rewrite the expression of the Hamming weight of a symmetric Boolean function $f$ of $n$ variables and of degree less than $2^\ell$, or equivalently of $\mathcal{F}(f)$

$$\mathcal{F}(f) = \sum_{i=0}^{n} (-1)^{v_i} \binom{n}{i} = \sum_{i=0}^{2^\ell - 1} (-1)^{v_i} \sum_{\substack{0 \le j \le n \\ j \equiv i \bmod 2^\ell}} \binom{n}{j}.$$

Using the formula of series multisection (see, for example, [13, p 84]), we get

$$\begin{aligned} A^L_n(i) &= \sum_{\substack{0 \le j \le n \\ j \equiv i \bmod L}} \binom{n}{j} \\ &= \frac{1}{L} \sum_{j=0}^{L-1} \left( 2 \cos\left( j \frac{\pi}{L} \right) \right)^n \cos\left( j(n-2i) \frac{\pi}{L} \right). \end{aligned}$$

TABLE I
CHARACTERISTICS OF THE QUADRATIC SYMMETRIC BOOLEAN FUNCTION WITH SIMPLIFIED ANF VECTOR $(0,\lambda,1,0,\ldots,0)$

| | $n\equiv 0 \bmod 4$ | $n\equiv 2 \bmod 4$ | $n\equiv 1 \bmod 4$ | $n\equiv 3 \bmod 4$ |
|---|---|---|---|---|
| $\mathcal{F}(f+\varphi_a)$ $wt(a)\equiv 0 \bmod 4$ | $(-1)^{\frac{n}{4}}2^{\frac{n}{2}}$ | $(-1)^{\lambda}(-1)^{\frac{n-2}{4}}2^{\frac{n}{2}}$ | $((-1)^{\lambda}+1)$ $\times(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}$ | $((-1)^{\lambda+1}+1)$ $\times(-1)^{\frac{n+1}{4}}2^{\frac{n-1}{2}}$ |
| $\mathcal{F}(f+\varphi_a)$ $wt(a)\equiv 1 \bmod 4$ | $(-1)^{\lambda+1}(-1)^{\frac{n}{4}}2^{\frac{n}{2}}$ | $(-1)^{\frac{n-2}{4}}2^{\frac{n}{2}}$ | $((-1)^{\lambda+1}+1)$ $\times(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}$ | $((-1)^{\lambda+1}-1)$ $\times(-1)^{\frac{n+1}{4}}2^{\frac{n-1}{2}}$ |
| $\mathcal{F}(f+\varphi_a)$ $wt(a)\equiv 2 \bmod 4$ | $(-1)^{\frac{n}{4}+1}2^{\frac{n}{2}}$ | $(-1)^{\lambda+1}(-1)^{\frac{n-2}{4}}2^{\frac{n}{2}}$ | $((-1)^{\lambda+1}-1)$ $\times(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}$ | $((-1)^{\lambda}-1)$ $\times(-1)^{\frac{n+1}{4}}2^{\frac{n-1}{2}}$ |
| $\mathcal{F}(f+\varphi_a)$ $wt(a)\equiv 3 \bmod 4$ | $(-1)^{\lambda}(-1)^{\frac{n}{4}}2^{\frac{n}{2}}$ | $(-1)^{\frac{n-2}{4}+1}2^{\frac{n}{2}}$ | $((-1)^{\lambda}-1)$ $\times(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}$ | $((-1)^{\lambda}+1)$ $\times(-1)^{\frac{n+1}{4}}2^{\frac{n-1}{2}}$ |
| $\mathcal{F}(D_af), a\notin\{0,\mathbf{1}\}$ | 0 | 0 | 0 | 0 |
| $\mathcal{F}(D_{\mathbf{1}}f)$ | 0 | 0 | $(-1)^{\lambda}2^n$ | $(-1)^{\lambda+1}2^n$ |

For $L=2^\ell$, the previous expression simplifies into

$$\begin{aligned}2^\ell A_n^{2^\ell}(i) &= \sum_{j=0}^{2^\ell-1}\left(2\cos\left(j\frac{\pi}{2^\ell}\right)\right)^n\cos\left(j(n-2i)\frac{\pi}{2^\ell}\right)\\ &= 2^n+\sum_{j=1}^{2^{\ell-1}-1}\left(2\cos\left(j\frac{\pi}{2^\ell}\right)\right)^n\cos\left(j(n-2i)\frac{\pi}{2^\ell}\right)\\ &\quad+\sum_{j=2^{\ell-1}-1}^{2^\ell-1}\left(-2\cos\left((2^\ell-j)\frac{\pi}{2^\ell}\right)\right)^n\\ &\quad\times\cos\left(j(n-2i)\frac{\pi}{2^\ell}\right).\end{aligned}$$

We transform the last term of the sum

$$\begin{aligned}&\sum_{j=2^{\ell-1}-1}^{2^\ell-1}\left(-2\cos\left((2^\ell-j)\frac{\pi}{2^\ell}\right)\right)^n\cos\left(j(n-2i)\frac{\pi}{2^\ell}\right)\\ &\quad=\sum_{k=1}^{2^{\ell-1}-1}\left(-2\cos\left(k\frac{\pi}{2^\ell}\right)\right)^n\cos\left((2^\ell-k)(n-2i)\frac{\pi}{2^\ell}\right).\end{aligned}$$

Using that

$$\begin{aligned}&\cos\left((2^\ell-k)(n-2i)\frac{\pi}{2^\ell}\right)\\ &\quad=\cos((n-2i)\pi)\cos\left(k(n-2i)\frac{\pi}{2^\ell}\right)\\ &\quad=(-1)^n\cos\left(k(n-2i)\frac{\pi}{2^\ell}\right)\end{aligned}$$

we finally get

$$\begin{aligned}A_n^{2^\ell}(i) &= 2^{n-\ell}\\ &\quad+2^{1-\ell}\sum_{j=1}^{2^{\ell-1}-1}\left(2\cos\left(j\frac{\pi}{2^\ell}\right)\right)^n\cos\left(j(n-2i)\frac{\pi}{2^\ell}\right).\end{aligned}\quad(2)$$

### A. Quadratic Symmetric Functions

All quadratic Boolean symmetric functions of $n$ variables can be described exhaustively. It is known that all quadratic symmetric functions of $n$ variables are bent if $n$ is even [5], and that their Walsh spectrum is three-valued and takes the values $\left\{0,\pm 2^{\frac{n+1}{2}}\right\}$ if $n$ is odd [6]. However, we are able to improve these results and to completely determine the characteristics of quadratic symmetric functions, especially the signs of their Walsh coefficients $\mathcal{F}(f+\varphi_a)$ as a function of $\mathrm{wt}(a)$ and of the ANF of $f$.

*Proposition 16:* Let $f\in\mathcal{B}_n$ be a symmetric function of degree 2, $n\geq 3$, with simplified ANF vector

$$\lambda(f)=(0,\lambda,1,0,\ldots,0),\qquad \lambda\in\boldsymbol{F}_2.$$

Then, its characteristics are given in the Table I.

Similarly, if we consider the quadratic function $g$ with simplified ANF vector $(1,\lambda,1,0,\ldots,0)$, i.e., $g=f+1$, we obviously deduce the characteristics of $g$ from Table I by

$$\mathcal{F}(g+\varphi_a)=-\mathcal{F}(f+\varphi_a)\quad\text{and}\quad\mathcal{F}(D_ag)=\mathcal{F}(D_af),\quad a\in\boldsymbol{F}_2^n.$$

*Proof:* Let $f\in\mathcal{B}_n$ be the symmetric function of degree 2 given by its simplified ANF vector $\lambda(f)=(0,\lambda,1,0,\ldots,0)$. From Theorem 1, its simplified value vector $v(f)$ is a part of $(0,\lambda,1,\lambda\oplus 1)^*$. First, we compute the Hamming weight of $f$. Since $v(f)$ is a part of $(0,\lambda,1,\lambda\oplus 1)^*$, we have

$$\begin{aligned}\mathcal{F}(f) &= A_n^4(0)+(-1)^\lambda A_n^4(1)-A_n^4(2)+(-1)^{\lambda+1}A_n^4(3)\\ &= A_n^4(0)-A_n^4(2)+(-1)^\lambda\left(A_n^4(1)-A_n^4(3)\right).\end{aligned}\quad(3)$$

Thanks to (2), we can derive the values of $A_n^4(i)$, $0\leq i\leq 3$ depending on $(n-2i) \bmod 4$

$$A_n^4(i)=\begin{cases}2^{n-2}+2^{\frac{n}{2}-1}(-1)^{\frac{n-2i}{4}}, & \text{if } n-2i\equiv 0 \bmod 4\\ 2^{n-2}+2^{\frac{n-3}{2}}(-1)^{\frac{n-2i-1}{4}}, & \text{if } n-2i\equiv 1 \bmod 4\\ 2^{n-2}, & \text{if } n-2i\equiv 2 \bmod 4\\ 2^{n-2}+2^{\frac{n-3}{2}}(-1)^{\frac{n-2i+1}{4}}, & \text{if } n-2i\equiv 3 \bmod 4.\end{cases}\quad(4)$$

Therefore, (3) leads to

$$\mathcal{F}(f)=\begin{cases}(-1)^{\frac{n}{4}}2^{\frac{n}{2}}, & \text{if } n\equiv 0 \bmod 4\\ ((-1)^\lambda+1)(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}, & \text{if } n\equiv 1 \bmod 4\\ (-1)^\lambda(-1)^{\frac{n-2}{4}}2^{\frac{n}{2}}, & \text{if } n\equiv 2 \bmod 4\\ ((-1)^{\lambda+1}+1)(-1)^{\frac{n+1}{4}}2^{\frac{n-1}{2}}, & \text{if } n\equiv 3 \bmod 4.\end{cases}$$

Now, we determine the Walsh coefficients of $f$ and their signs. First, we deduce from [10, Theorem V.1] that

$$\mathcal{F}(f)+\mathcal{F}(f+\varphi_{e_n})=2\mathcal{F}(f_H)$$

TABLE II
VALUES OF $\mathcal{F}(f)$, WHEN $f$ IS A CUBIC SYMMETRIC BOOLEAN FUNCTION

| $\mathcal{F}(f)$ | $n \equiv 0 \bmod 4$ | $n \equiv 2 \bmod 4$ | $n \equiv 1 \bmod 4$ | $n \equiv 3 \bmod 4$ |
|---|---|---|---|---|
| $\lambda(f) = (00010\ldots0)$ | $2^{n-1}$ | $2^{n-1} + (-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}}$ | $2^{n-1} + (-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}}$ | $2^{n-1} - (-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}}$ |
| $\lambda(f) = (01010\ldots0)$ | $2^{n-1}$ | $2^{n-1} - (-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}}$ | $2^{n-1} - (-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}}$ | $2^{n-1} + (-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}}$ |
| $\lambda(f) = (00110\ldots0)$ | $2^{n-1} + (-1)^{\frac{n}{4}} 2^{\frac{n}{2}}$ | $2^{n-1}$ | $2^{n-1} + (-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}}$ | $2^{n-1} + (-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}}$ |
| $\lambda(f) = (01110\ldots0)$ | $-2^{n-1} + (-1)^{\frac{n}{4}} 2^{\frac{n}{2}}$ | $-2^{n-1}$ | $-2^{n-1} + (-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}}$ | $-2^{n-1} + (-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}}$ |

where $f_H$ is the function of $(n-1)$ variables corresponding to the restriction of $f$ to the hyperplane $H = \langle e_1, \ldots, e_{n-1} \rangle$. We know from Proposition 7 that $f_H$ is symmetric and that its simplified ANF vector is $\lambda(f_H) = (0, \lambda, 1, 0, \ldots, 0)$. Then, $f_H$ is quadratic when $n \geq 3$, and its weight can be derived from the previous formulae. This leads to

$$\mathcal{F}(f + \varphi_{e_n}) = \begin{cases} (-1)^{\frac{n}{4}+\lambda+1} 2^{\frac{n}{2}}, & \text{if } n \equiv 0 \bmod 4 \\ ((-1)^{\lambda+1} + 1)(-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}}, & \text{if } n \equiv 1 \bmod 4 \\ (-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}}, & \text{if } n \equiv 2 \bmod 4 \\ ((-1)^{\lambda+1} - 1)(-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}}, & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

When $n$ is even, $f$ is bent. Then, all its Walsh coefficients are equal to $\pm 2^{\frac{n}{2}}$ and their signs are given by the *dual function*, $\widetilde{f}$ [19]

$$\mathcal{F}(f + \varphi_a) = (-1)^{\widetilde{f}(a)} 2^{\frac{n}{2}}.$$

Since $\mathcal{F}(f + \varphi_a)$ only depends on the weight of $a$ (Proposition 3), the dual of $f$ is symmetric. Moreover, the dual of a quadratic bent function is quadratic as well [19, p. 87]. Then, the simplified value vector of the dual function is a part of $(v_0, v_1, v_0 \oplus 1, v_1 \oplus 1)^*$ where $v_0$ and $v_1$, respectively, correspond to the signs of $\mathcal{F}(f)$ and $\mathcal{F}(f + \varphi_{e_n})$. It follows that, for any $\alpha$ and $\beta$ in $\boldsymbol{F}_2^n$ such that $\mathrm{wt}(\alpha) \equiv \mathrm{wt}(\beta) + 2 \bmod 4$

$$\mathcal{F}(f + \varphi_\alpha) = -\mathcal{F}(f + \varphi_\beta).$$

When $n$ is odd, $\mathcal{F}(f + \varphi_a)$ can be computed as follows. For $a \neq \mathbf{1}$, we choose $b$ of weight 1 such that $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$. For $H = \{0, b\}^\perp$ we consider $(f_H, f_{\bar{H}})$ the decomposition of $f$ with respect to $H$. From Proposition 7, we have $\lambda(f_H) = (0, \lambda, 1, 0, \ldots, 0)$ and $\lambda(f_{\bar{H}}) = (\lambda, \lambda \oplus 1, 1, 0, \ldots, 0)$. Moreover

$$\begin{aligned} \mathcal{F}(f + \varphi_a) &= \sum_{x \in H} (-1)^{f(x)+a\cdot x} + \sum_{x \in \bar{H}} (-1)^{f(x)+a\cdot x} \\ &= \mathcal{F}(f_H + \varphi_a) + \mathcal{F}(f_{\bar{H}} + \varphi_a). \end{aligned}$$

Since both $f_H$ and $f_{\bar{H}}$ are symmetric quadratic bent functions, we deduce that, for any $\alpha, \beta \in H$ such that $\mathrm{wt}(\alpha) \equiv \mathrm{wt}(\beta) + 2 \bmod 4$, we have

$$\begin{aligned} \mathcal{F}(f + \varphi_\alpha) &= \mathcal{F}(f_H + \varphi_\alpha) + \mathcal{F}(f_{\bar{H}} + \varphi_\alpha) \\ &= -\mathcal{F}(f_H + \varphi_\beta) - \mathcal{F}(f_{\bar{H}} + \varphi_\beta) \\ &= -\mathcal{F}(f + \varphi_\beta). \end{aligned}$$

The value of $\mathcal{F}(f + \varphi_{\mathbf{1}})$ can be derived from the previous calculations since the simplified ANF vector of $f + \varphi_{\mathbf{1}}$ is $(0, \lambda \oplus 1, 1, 0, \ldots, 0)$. By replacing $\lambda$ by $\lambda \oplus 1$ in the value of $\mathcal{F}(f)$, we see that $\mathcal{F}(f + \varphi_{\mathbf{1}}) = \mathcal{F}(f + \varphi_a)$ with $\mathrm{wt}(a) \equiv n \bmod 4$.

Finally, the weights of the derivatives can be easily obtained. When $n$ is even, $f$ is bent, implying that $\mathcal{F}(D_a f) = 0$ for all $a \in \boldsymbol{F}_2^n$. When $n$ is odd, $D_a f$ has degree 1 (implying that it is balanced) for all $a \neq \mathbf{1}$ (Corollary 4). Moreover, we have $\deg(D_{\mathbf{1}} f) < 1$ (Proposition 15). Then $D_{\mathbf{1}} f$ is constant and its value is given by Proposition 14

$$\lambda_{D_{\mathbf{1}} f}(0) = \bigoplus_{k \preceq n, k \neq 0} \lambda_f(k) = \begin{cases} \lambda, & \text{if } n \equiv 1 \bmod 4 \\ \lambda \oplus 1, & \text{if } n \equiv 3 \bmod 4. \end{cases}$$ □

### B. Cubic Symmetric Functions

Now, we determine all characteristics of symmetric functions of degree 3. They are summarized in the following propositions. The first one determines the Hamming weights of all cubic symmetric functions. Most notably, it points out that balanced symmetric functions of degree 3 do not exist.

*Proposition 17:* The Hamming weights of the symmetric functions $f \in \mathcal{B}_n$ of degree 3 are determined by Table II.

*Proof:* Let $f \in \mathcal{B}_n$ be a symmetric function of degree 3 with simplified ANF vector $\lambda(f) = (0, \lambda_1, \lambda_2, 1, 0, \ldots, 0)$. Thanks to Theorem 1, we know that its simplified value vector $v(f)$ is periodic with period 4 and that it is a part of $(0, \lambda_1, \lambda_2, \lambda_1 \oplus \lambda_2 \oplus 1)^*$. Therefore,

$$\begin{aligned} \mathcal{F}(f) = A_n^4(0) &+ (-1)^{\lambda_1} A_n^4(1) \\ &+ (-1)^{\lambda_2} A_n^4(2) + (-1)^{\lambda_1+\lambda_2+1} A_n^4(3). \end{aligned}$$

The result then is directly deduced from the values of $A_n^4(i)$ given by (4). □

The previous study of quadratic symmetric functions can be used to calculate the weights of the derivatives of a cubic symmetric function.

*Proposition 18:* Let $f \in \mathcal{B}_n$ be a symmetric function of degree 3 with simplified ANF vector

$$\lambda(f) = (0, \lambda_1, \lambda_2, 1, 0, \ldots, 0).$$

Then, the Hamming weights of its derivatives are given in the Table III.

*Proof:* From Proposition 11, we can restrict ourselves to the derivatives with respect to $a = e_{n-k+1} + \cdots + e_n$ for $0 \leq k \leq n$. We use the same notation as in Proposition 12. Let $V = \langle e_1, \ldots, e_{n-k} \rangle$ and $\overline{V} = \langle e_{n-k+1}, \ldots, e_n \rangle$. All the restrictions

TABLE III
VALUES OF $\mathcal{F}(D_a f)$ WHEN $f$ IS A CUBIC SYMMETRIC BOOLEAN FUNCTION WITH SIMPLIFIED ANF VECTOR $\lambda(f) = (0, \lambda_1, \lambda_2, 1, 0, \ldots, 0)$

| $\mathcal{F}(D_a f)$ | $n \equiv 0 \bmod 4$ | $n \equiv 2 \bmod 4$ | $n \equiv 1 \bmod 4$ | $n \equiv 3 \bmod 4$ |
|---|---|---|---|---|
| $wt(a) \equiv 0 \bmod 4,\ a \neq 0$ | $2^{n-1}$ | $2^{n-1}$ | $2^{n-1}$ | $2^{n-1}$ |
| $wt(a) \equiv 1 \bmod 4,\ a \neq \mathbf{1}$ | $(1+(-1)^{\lambda_2+1})$ $\times(-1)^{\frac{n}{4}+\lambda_1}2^{\frac{n}{2}}$ | $(1+(-1)^{\lambda_2})$ $\times(-1)^{\frac{n-2}{4}+\lambda_1}2^{\frac{n}{2}}$ | $(-1)^{\frac{n-1}{4}+\lambda_1}2^{\frac{n+1}{2}}$ | $(-1)^{\lambda_1+\lambda_2}$ $(-1)^{\frac{n-3}{4}}2^{\frac{n+1}{2}}$ |
| $wt(a) \equiv 2 \bmod 4,\ a \neq \mathbf{1}$ | $2^{n-1}$ | $2^{n-1}$ | $2^{n-1}$ | $2^{n-1}$ |
| $wt(a) \equiv 3 \bmod 4,\ a \neq \mathbf{1}$ | $(1+(-1)^{\lambda_2+1})$ $\times(-1)^{\frac{n}{4}+\lambda_1}2^{\frac{n}{2}}$ | $(1+(-1)^{\lambda_2})$ $\times(-1)^{\frac{n-2}{4}+\lambda_1}2^{\frac{n}{2}}$ | $(-1)^{\frac{n-1}{4}+\lambda_1}2^{\frac{n+1}{2}}$ | $(-1)^{\lambda_1+\lambda_2}$ $(-1)^{\frac{n-3}{4}}2^{\frac{n+1}{2}}$ |
| $a = \mathbf{1}$ | $(1+(-1)^{\lambda_2+1})2^{n-1}$ | $(1+(-1)^{\lambda_2})2^{n-1}$ | $(-1)^{\frac{n-1}{4}+\lambda_1}2^{\frac{n+1}{2}}$ | $(-1)^{\lambda_1+\lambda_2}$ $(-1)^{\frac{n-3}{4}}2^{\frac{n+1}{2}}$ |

$g_b$, $b \in \overline{V}$, of $D_a f$ to $b+V$ are symmetric and only depends on $\mathrm{wt}(b)$. Their simplified ANF vectors are (see Proposition 12)

$$\lambda_{g_b}(i) = \bigoplus_{j \preceq k-\mathrm{wt}(b)} \lambda_f(i+j) \oplus \bigoplus_{j \preceq \mathrm{wt}(b)} \lambda_f(i+j).$$

As for all $i, j$ such that $i+j > 3$, $\lambda_f(i+j) = 0$, $k$ and $\mathrm{wt}(b)$ can be considered modulo 4: only their last two bits are involved in the previous formula. This gives the following algebraic normal form for $g_b$:

- if $\mathrm{wt}(b) \equiv 0 \bmod 4$

$$\lambda(g_b) = \begin{cases} (0,0,0,\ldots), & \text{if } k \equiv 0 \bmod 4 \\ (\lambda_1, \lambda_2, 1, 0, \ldots), & \text{if } k \equiv 1 \bmod 4 \\ (\lambda_2, 1, 0, \ldots), & \text{if } k \equiv 2 \bmod 4 \\ (\lambda_1 \oplus \lambda_2 \oplus 1, \lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 3 \bmod 4; \end{cases}$$

- if $\mathrm{wt}(b) \equiv 1 \bmod 4$

$$\lambda(g_b) = \begin{cases} (\lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 0 \bmod 4 \\ (\lambda_1, \lambda_2, 1, 0, \ldots), & \text{if } k \equiv 1 \bmod 4 \\ (0,0,0,\ldots), & \text{if } k \equiv 2 \bmod 4 \\ (\lambda_1 \oplus \lambda_2, \lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 3 \bmod 4; \end{cases}$$

- if $\mathrm{wt}(b) \equiv 2 \bmod 4$

$$\lambda(g_b) = \begin{cases} (0,0,0,\ldots), & \text{if } k \equiv 0 \bmod 4 \\ (\lambda_1 \oplus 1, \lambda_2, 1, 0, \ldots), & \text{if } k \equiv 1 \bmod 4 \\ (\lambda_2, 1, 0, \ldots), & \text{if } k \equiv 2 \bmod 4 \\ (\lambda_1 \oplus \lambda_2, \lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 3 \bmod 4; \end{cases}$$

- if $\mathrm{wt}(b) \equiv 3 \bmod 4$

$$\lambda(g_b) = \begin{cases} (\lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 0 \bmod 4 \\ (\lambda_1 \oplus 1, \lambda_2, 1, 0, \ldots), & \text{if } k \equiv 1 \bmod 4 \\ (0,0,0,\ldots), & \text{if } k \equiv 2 \bmod 4 \\ (\lambda_1 \oplus \lambda_2 \oplus 1, \lambda_2 \oplus 1, 1, 0, \ldots), & \text{if } k \equiv 3 \bmod 4. \end{cases}$$

We deduce that, for $a = e_{n-k+1} + \cdots + e_n$

$$\begin{aligned} \mathcal{F}(D_a f) &= \sum_{b \in \overline{V}} \mathcal{F}(g_b) \\ &= \sum_{\beta=0}^{k} \binom{k}{\beta} \mathcal{F}(g_{e_{n-\beta+1}+\cdots+e_n}) \\ &= \sum_{i=0}^{4} \mathcal{F}(g_{e_{n-i+1}+\cdots+e_n}) A_k^4(i). \end{aligned}$$

When $k$ is even, all restrictions $g_b$ are constant or linear functions. Thus, we deduce

$$\mathcal{F}(D_a f) = \begin{cases} 2^{n-k}\left(A_k^4(0) + A_k^4(2)\right) = 2^{n-1}, & \text{if } k \equiv 0 \bmod 4 \\ 2^{n-k}\left(A_k^4(1) + A_k^4(3)\right) = 2^{n-1}, & \text{if } k \equiv 2 \bmod 4. \end{cases}$$

When $k$ is odd, we have

- if $k \equiv 1 \bmod 4$

$$\begin{aligned} \mathcal{F}(D_a f) &= \mathcal{F}(g_0)\left(A_k^4(0) + A_k^4(1) - A_k^4(2) - A_k^4(3)\right) \\ &= \mathcal{F}(g_0)(-1)^{\frac{k-1}{4}}2^{\frac{k+1}{2}}; \end{aligned}$$

- if $k \equiv 3 \bmod 4$

$$\begin{aligned} \mathcal{F}(D_a f) &= \mathcal{F}(g_0)\left(A_k^4(0) - A_k^4(1) - A_k^4(2) + A_k^4(3)\right) \\ &= \mathcal{F}(g_0)(-1)^{\frac{k+1}{4}}2^{\frac{k+1}{2}} \end{aligned}$$

and the value of $\mathcal{F}(g_0)$ can be deduced from Proposition 16 since $g_0$ is a quadratic symmetric function of $(n-k)$ variables.

Finally, Proposition 14 enables to compute the weight of $D_{\mathbf{1}} f$: for all $0 \leq i \leq 2$

$$\lambda_{D_{\mathbf{1}} f}(i) = \bigoplus_{\substack{k \preceq n-i \\ k \neq 0}} \lambda_f(k+i).$$

It leads to the following simplified ANF vectors for $D_{\mathbf{1}} f$:

$$\lambda(D_{\mathbf{1}} f) = \begin{cases} (0, \lambda_2 \oplus 1, 0, \ldots, 0), & \text{if } n \equiv 0 \bmod 4 \\ (\lambda_2, \lambda_2, 0, \ldots, 0), & \text{if } n \equiv 2 \bmod 4 \\ (\lambda_1, 0, 1, 0, \ldots, 0), & \text{if } n \equiv 1 \bmod 4 \\ (\lambda_1 \oplus \lambda_2 \oplus 1, 1, 1, 0, \ldots, 0), & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

The corresponding weights are derived from Proposition 16. □

Finally, we are able to determine the whole Walsh spectra of symmetric functions of degree 3 from the weights of their derivatives.

*Proposition 19:* Let $f \in \mathcal{B}_n$ be a symmetric function of degree 3 with simplified ANF vector

$$\lambda(f) = (0, \lambda_1, \lambda_2, 1, 0, \ldots, 0).$$

Then, for any $a \in \boldsymbol{F}_2^n$, $a \notin \{0, \mathbf{1}\}$, we have

$$|\mathcal{F}(f+\varphi_a)| = \begin{cases} 2^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ 2^{\frac{n}{2}-1}|1+(-1)^{\lambda_2+\mathrm{wt}(a)+1}|, & \text{if } n \equiv 0 \bmod 4 \\ 2^{\frac{n}{2}-1}|1+(-1)^{\lambda_2+\mathrm{wt}(a)}|, & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

Moreover, the nonlinearity of $f$ is $\mathcal{N}_f = 2^{n-1} - \frac{\mathcal{L}(f)}{2}$ where

$$\mathcal{L}(f) = \max\left(|\mathcal{F}(f)|, |\mathcal{F}(f+\varphi_{\mathbf{1}})|\right) = \begin{cases} 2^{n-1}, & \text{if } n+2\lambda_2 \equiv 0 \bmod 4 \\ 2^{n-1}+2^{\frac{n}{2}}, & \text{if } n+2\lambda_2 \equiv 2 \bmod 4 \\ 2^{n-1}+2^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

*Proof:* We apply [10, Theorem V.1] to the hyperplane $H_{\mathbf{1}} = \{0, \mathbf{1}\}^{\perp}$, corresponding to the set of the vectors of even weight: for any $b \notin \{0, \mathbf{1}\}$

$$\mathcal{F}^2(f+\varphi_b) + \mathcal{F}^2(f+\varphi_{b+\mathbf{1}}) = 2\sum_{e \in H_{\mathbf{1}}} (-1)^{b \cdot e} \mathcal{F}(D_e f).$$

We know from Proposition 18 that, for $e \in H_{\mathbf{1}}$, $e \neq 0, \mathbf{1}$, we have $\mathcal{F}(D_e f) = 2^{n-1}$.

When $n$ is odd, $\mathbf{1}$ does not belong to $H_{\mathbf{1}}$. Therefore, we obtain

$$\begin{aligned} &\mathcal{F}^2(f+\varphi_b) + \mathcal{F}^2(f+\varphi_{b+\mathbf{1}}) \\ &\quad = 2\left(2^{n-1} \sum_{e \in H_{\mathbf{1}},\, e \neq 0} (-1)^{b \cdot e} + \mathcal{F}(D_0 f)\right) \\ &\quad = 2(-2^{n-1} + 2^n) = 2^n \end{aligned}$$

implying that $\mathcal{F}^2(f+\varphi_b) = 2^{n-1}$ for any $b \neq 0, \mathbf{1}$ (see, e.g., [10, Lemma B.1]).

When $n$ is even, we have to add the term $\mathcal{F}(D_{\mathbf{1}} f)$ which depends on $n \bmod 4$. In this case, we have

$$\begin{aligned} &\mathcal{F}^2(f+\varphi_b) + \mathcal{F}^2(f+\varphi_{b+\mathbf{1}}) \\ &\quad = 2^n \sum_{e \in H_{\mathbf{1}} \setminus \{0, \mathbf{1}\}} (-1)^{b \cdot e} \\ &\qquad + 2\left(\mathcal{F}(D_0 f) + (-1)^{\mathrm{wt}(b)} \mathcal{F}(D_{\mathbf{1}} f)\right) \\ &\quad = 2^n \left(1 + (-1)^{\mathrm{wt}(b)+1}\right) + (-1)^{\mathrm{wt}(b)} 2\mathcal{F}(D_{\mathbf{1}} f) \\ &\quad = 2^n \left(1 + (-1)^{\lambda_2+1+\mathrm{wt}(b)}\right), \quad \text{if } n \equiv 0 \bmod 4 \\ &\quad = 2^n \left(1 + (-1)^{\lambda_2+\mathrm{wt}(b)}\right), \quad \text{if } n \equiv 2 \bmod 4. \end{aligned}$$

From [10, Lemma B.1], we deduce that for all $b \neq 0, \mathbf{1}$

$$|\mathcal{F}(f+\varphi_b)| = \begin{cases} 2^{\frac{n}{2}-1}\left(1+(-1)^{\lambda_2+1+\mathrm{wt}(b)}\right), & \text{if } n \equiv 0 \bmod 4 \\ 2^{\frac{n}{2}-1}\left(1+(-1)^{\lambda_2+\mathrm{wt}(b)}\right), & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

The values of $\mathcal{F}(f)$ and of $\mathcal{F}(f+\varphi_{\mathbf{1}})$ are given by Proposition 17 (note that the simplified ANF vector of $f+\varphi_{\mathbf{1}}$ is $(0, \lambda_1 \oplus 1, \lambda_2, 1, \ldots, 0)$). Then, we can notice that

$$\mathcal{L}(f) = \max\left(|\mathcal{F}(f)|, |\mathcal{F}(f+\varphi_{\mathbf{1}})|\right). \qquad \square$$

### C. Hamming Weights of Symmetric Functions of Degree Less Than 8

We are now interested in the symmetric functions of degree at most 7. Most notably, we want to determine if there exist balanced symmetric functions of degree at most 7 for any number of variables. When $\deg(f) \leq 7$, the simplified value vector of $f$ is a part of $(v_0, v_1, \ldots, v_7)^*$ for some $(v_0, \ldots, v_7) \in \boldsymbol{F}_2^8$. Therefore,

$$\mathcal{F}(f) = \sum_{i=0}^{7} (-1)^{v_i} A_n^8(i)$$

where $A_n^8(i)$ is given in (2). Thus,

$$\mathcal{F}(f) = 2^{n-3} \sum_{i=0}^{7} (-1)^{v_i} + \frac{1}{4} \sum_{j=1}^{3} \left(2\cos\left(j\frac{\pi}{8}\right)\right)^n \sum_{i=0}^{7} (-1)^{v_i} \cos\left(j(n-2i)\frac{\pi}{8}\right).$$

We know that

$$\cos\left(\frac{\pi}{8}\right) = \sqrt{\frac{1}{2} + \frac{1}{2\sqrt{2}}} \text{ and } \cos\left(\frac{3\pi}{8}\right) = \sqrt{\frac{1}{2} - \frac{1}{2\sqrt{2}}}.$$

First, we focus on the weights of the symmetric functions of degree at most 7 which depend on an even number of variables $n = 2t$. Then, we obtain

$$\begin{aligned} \mathcal{F}(f) = {} & 2^{2t-3} \sum_{i=0}^{7} (-1)^{v_i} \\ & + 2^{t-2} \sum_{i=0}^{7} (-1)^{v_i} \cos\left((t-i)\frac{\pi}{2}\right) \\ & + \frac{1}{4}(2+\sqrt{2})^t \sum_{i=0}^{7} (-1)^{v_i} \cos\left((t-i)\frac{\pi}{4}\right) \\ & + \frac{1}{4}(2-\sqrt{2})^t \sum_{i=0}^{7} (-1)^{v_i} \cos\left((t-i)\frac{3\pi}{4}\right). \end{aligned}$$

As the angles have to be considered modulo $2\pi$, the values of the respective cosines only depend on $(t-i) \bmod 8$. We can combine this property with the periodicity of $v(f)$, which has period 8 and we obtain

$$\begin{aligned} \mathcal{F}(f) = {} & 2^{2t-3} \sum_{i=0}^{7} (-1)^{v_i} + 2^{t-2} \sum_{i=0}^{7} (-1)^{v_{t-i}} \cos\left(i\frac{\pi}{2}\right) \\ & + \frac{1}{4}(2+\sqrt{2})^t \sum_{i=0}^{7} (-1)^{v_{t-i}} \cos\left(i\frac{\pi}{4}\right) \\ & + \frac{1}{4}(2-\sqrt{2})^t \sum_{i=0}^{7} (-1)^{v_{t-i}} \cos\left(i\frac{3\pi}{4}\right) \end{aligned}$$

where the indices in $v_{t-i}$ are considered modulo 8. Therefore,

$$\begin{aligned}\mathcal{F}(f) = 2^{2t-3}&\sum_{i=0}^{7}(-1)^{v_i}\\ &+2^{t-2}\left((-1)^{v_t}-(-1)^{v_{t-2}}+(-1)^{v_{t-4}}-(-1)^{v_{t-6}}\right)\\ &+\frac{1}{4\sqrt{2}}\left((2+\sqrt{2})^t-(2-\sqrt{2})^t\right)\\ &\times\left((-1)^{v_{t-1}}-(-1)^{v_{t-3}}-(-1)^{v_{t-5}}+(-1)^{v_{t-7}}\right)\\ &+\frac{1}{4}\left((2+\sqrt{2})^t+(2-\sqrt{2})^t\right)\\ &\times\left((-1)^{v_t}-(-1)^{v_{t-4}}\right).\end{aligned}$$

In the following, we use the notation, $\forall\, k \geq 0$

$$\begin{aligned}D_k^+ &= \frac{1}{2}\left((2+\sqrt{2})^k+(2-\sqrt{2})^k\right)\\ D_k^- &= \frac{1}{2\sqrt{2}}\left((2+\sqrt{2})^k-(2-\sqrt{2})^k\right)\end{aligned} \tag{5}$$

and

$$\begin{aligned}A(a,b,c,d) &= (-1)^a+(-1)^b+(-1)^c+(-1)^d\\ B(a,b,c,d) &= (-1)^a+(-1)^b+(-1)^{c+1}+(-1)^{d+1}\end{aligned} \tag{6}$$

for any $(a,b,c,d) \in \boldsymbol{F}_2^4$. Then

$$\begin{aligned}\mathcal{F}(f) = 2^{2t-3}&(A(v_t,v_{t-4},v_{t-2},v_{t-6})\\ &\quad+A(v_{t-1},v_{t-7},v_{t-3},v_{t-5}))\\ &+2^{t-2}B(v_t,v_{t-4},v_{t-2},v_{t-6})\\ &+\frac{1}{2}D_t^-B(v_{t-1},v_{t-7},v_{t-3},v_{t-5})\\ &+\frac{1}{2}D_t^+\left((-1)^{v_t}-(-1)^{v_{t-4}}\right).\end{aligned} \tag{7}$$

Now, we want to determine the symmetric functions in $\mathcal{B}_{2t}$ of degree at most 7 which are balanced. We need the following lemma.

*Lemma 2:* For any $n \geq 3$, we have

$$2^{n-1+\lceil\frac{n}{2}\rceil} < D_n^+$$

and for any $n \geq 14$

$$2^{n-1+\lfloor\frac{n}{2}\rfloor} < D_n^- < 2^{2n-5}+2^{2n-6}.$$

*Proof:* By definition, we have

$$\begin{aligned}D_n^+ &= \frac{1}{2}\left((2+\sqrt{2})^n+(2-\sqrt{2})^n\right)\\ &= \sum_{\substack{0\leq i\leq n\\ i\ \text{even}}}\binom{n}{i}2^{n-\frac{i}{2}}.\end{aligned}$$

It follows that

$$D_n^+ > 2^{n-\lfloor\frac{n}{2}\rfloor}\sum_{\substack{0\leq i\leq n\\ i\ \text{even}}}\binom{n}{i} \geq 2^{n-1}\cdot 2^{\lceil\frac{n}{2}\rceil},$$

for any $n \geq 2$.

A similar computation for $D_n^-$ leads to

$$\begin{aligned}D_n^- &= \frac{1}{2\sqrt{2}}\left((2+\sqrt{2})^n-(2-\sqrt{2})^n\right)\\ &= \sum_{\substack{0\leq i\leq n\\ i\ \text{odd}}}\binom{n}{i}2^{n-\frac{i+1}{2}}.\end{aligned}$$

Then

$$D_n^- > 2^{n-\lceil\frac{n}{2}\rceil}\sum_{\substack{0\leq i\leq n\\ i\ \text{odd}}}\binom{n}{i} \geq 2^{n-1}\cdot 2^{\lfloor\frac{n}{2}\rfloor}$$

for any $n \geq 3$. Moreover

$$\begin{aligned}D_n^- &= n\cdot 2^{n-1}+\binom{n}{3}2^{n-2}+\binom{n}{5}2^{n-3}+\sum_{\substack{7\leq i\leq n\\ i\ \text{odd}}}\binom{n}{i}2^{n-\frac{i+1}{2}}\\ &\leq n\cdot 2^{n-1}+\binom{n}{3}2^{n-2}+\binom{n}{5}2^{n-3}\\ &\quad+2^{n-4}\left(2^{n-1}-n-\binom{n}{3}-\binom{n}{5}\right)\\ &\leq 2^{2n-5}+2^{n-4}\left(7n+3\binom{n}{3}+\binom{n}{5}\right).\end{aligned}$$

Since $7n+3\binom{n}{3}+\binom{n}{5} < 2^{n-2}$ for any $n \geq 14$, we obtain that

$$D_n^- < 2^{2n-5}+2^{2n-6}. \qquad \square$$

*Theorem 4:* For any even $n \geq 2$, there is no balanced symmetric Boolean function of $n$ variables of degree less than or equal to 7 except the functions of degree 1 and the functions of eight variables with simplified ANF vectors

$$\lambda(f) = (\varepsilon,1,1,0,0,0,0,1,0) \quad \text{and} \quad \lambda(f) = (\varepsilon,1,1,1,0,1,0,1,0).$$

*Proof:* For any symmetric function $f \in \mathcal{B}_n$ with $n = 2t$ even and $\deg(f) \leq 7$, we have from (7)

$$\begin{aligned}\mathcal{F}(f) = 2^{2t-3}&(A_1+A_2)+2^{t-2}B_1\\ &+\frac{1}{2}D_t^-B_2+\frac{1}{2}D_t^+\left((-1)^{v_t}+(-1)^{v_{t-4}+1}\right)\end{aligned}$$

where

$$\begin{cases}A_1 = A(v_t,v_{t-4},v_{t-2},v_{t-6})\\ B_1 = B(v_t,v_{t-4},v_{t-2},v_{t-6})\end{cases}$$

and

$$\begin{cases}A_2 = A(v_{t-1},v_{t-7},v_{t-3},v_{t-5})\\ B_2 = B(v_{t-1},v_{t-7},v_{t-3},v_{t-5}).\end{cases}$$

We have to distinguish the following cases.

- If $A_1+A_2 \neq 0$, then $|A_1+A_2| \geq 2$. It follows that either

$$\mathcal{F}(f) \geq 2^{2t-2}-2^t-D_t^+-2D_t^-$$

or

$$\mathcal{F}(f) \leq -2^{2t-2} + 2^t + D_t^+ + 2D_t^-.$$

Using that for any $k > 0$, $D_k^+ + 2D_k^- = D_{k+1}^-$, we deduce that

$$|\mathcal{F}(f)| \geq 2^{2t-2} - 2^t - D_{t+1}^- > 0$$

for any $t \geq 14$ where the last inequality is derived from Lemma 2.

- If $A_1 + A_2 = 0$ and $B_1 \neq 0$, we have

$$|\mathcal{F}(f)| \geq \frac{1}{2}\left|D_t^+\left((-1)^{v_t} + (-1)^{v_{t-4}+1}\right) + D_t^- B_2\right| - 2^t.$$

It follows that for $v_t = v_{t-4}$ and $B_2 \neq 0$

$$\mathcal{F}(f) \geq D_t^- - 2^t > 0.$$

For $v_t = v_{t-4}$ and $B_2 = 0$, we obviously have

$$|\mathcal{F}(f)| = 2^{t-2}|B_1| > 0.$$

For $v_t \neq v_{t-4}$, we have

$$\left|D_t^+ + \frac{1}{2}D_t^- B_2\right| \geq \left|D_t^+ - 2D_t^-\right| = 2D_{t-1}^- > 2^t.$$

- If $A_1 + A_2 = 0$ and $B_1 = 0$, we have

$$\mathcal{F}(f) = \frac{1}{2}D_t^+\left((-1)^{v_t} + (-1)^{v_{t-4}+1}\right) + \frac{1}{2}D_t^- B_2.$$

If $v_t \neq v_{t-4}$

$$|\mathcal{F}(f)| \geq \left|D_t^+ - 2D_t^-\right| = 2D_{t-1}^- > 0.$$

If $v_t = v_{t-4}$, we obtain $\mathcal{F}(f) = \frac{1}{2}D_t^- B_2$. But, $v_t = v_{t-4}$, $B_1 = B_2 = 0$, and $A_1 + A_2 = 0$ occur if and only if $v_i = \varepsilon$ when $i$ is even and $v_i = \varepsilon \oplus 1$ when $i$ is odd. This means that $v(f)$ is a part of $(0,1)^*$ or of $(1,0)^*$, i.e., that $f$ has degree 1.

Then, we have proved that for any even $n \geq 28$, a symmetric function $f \in \mathcal{B}_n$ with $\deg(f) \leq 7$ is balanced if and only if $\deg(f) = 1$. By computing all possible values of $\mathcal{F}(f)$ for the symmetric functions of $n$ variables when $n$ is even and less than 28, we finally check that the only balanced symmetric functions are the functions of degree 1 and the functions of eight variables defined by the following simplified ANF vectors:

$$\lambda(f) = (\varepsilon, 1, 1, 0, 0, 0, 0, 1, 0)$$
$$\text{and} \quad \lambda(f) = (\varepsilon, 1, 1, 1, 0, 1, 0, 1, 0). \quad \square$$

Now, we focus on the symmetric functions of degree at most 7 which depend on an odd number of variables $n = 2t+1$. We can rewrite the expression of $\mathcal{F}(f)$

$$\begin{aligned}
\mathcal{F}(f) = {} & 2^{2t-2}\sum_{i=0}^{7}(-1)^{v_i} \\
& + 2^{t-2}\sqrt{2}\sum_{i=0}^{7}(-1)^{v_i}\cos\left((t-i)\frac{\pi}{2} + \frac{\pi}{4}\right) \\
& + \frac{1}{4}\left(2+\sqrt{2}\right)^{t+\frac{1}{2}}\sum_{i=0}^{7}(-1)^{v_i}\cos\left((t-i)\frac{\pi}{4} + \frac{\pi}{8}\right) \\
& + \frac{1}{4}\left(2-\sqrt{2}\right)^{t+\frac{1}{2}}\sum_{i=0}^{7}(-1)^{v_i} \\
& \times \cos\left((t-i)\frac{3\pi}{4} + \frac{3\pi}{8}\right) \\
= {} & 2^{2t-2}\sum_{i=0}^{7}(-1)^{v_i} \\
& + 2^{t-2}\sqrt{2}\sum_{i=0}^{7}(-1)^{v_{t-i}}\cos\left(i\frac{\pi}{2} + \frac{\pi}{4}\right) \\
& + \frac{1}{4}\left(2+\sqrt{2}\right)^{t+\frac{1}{2}}\sum_{i=0}^{7}(-1)^{v_{t-i}}\cos\left(i\frac{\pi}{4} + \frac{\pi}{8}\right) \\
& + \frac{1}{4}\left(2-\sqrt{2}\right)^{t+\frac{1}{2}}\sum_{i=0}^{7}(-1)^{v_{t-i}}\cos\left(i\frac{3\pi}{4} + \frac{3\pi}{8}\right)
\end{aligned}$$

where the last equality comes from the fact that $(t-i)$ can be considered modulo 8 and that the simplified value vector of $f$ has period 8. By expanding the previous sums, we obtain

$$\begin{aligned}
\mathcal{F}(f) = {} & 2^{2t-2}\sum_{i=0}^{7}(-1)^{v_i} \\
& + 2^{t-2}((-1)^{v_t} - (-1)^{v_{t-1}} - (-1)^{v_{t-2}} + (-1)^{v_{t-3}} \\
& \quad + (-1)^{v_{t-4}} - (-1)^{v_{t-5}} \\
& \quad - (-1)^{v_{t-6}} + (-1)^{v_{t-7}}) \\
& + \frac{1}{4}\left((2+\sqrt{2})^{t+\frac{1}{2}}\cos\frac{\pi}{8} + (2-\sqrt{2})^{t+\frac{1}{2}}\cos\frac{3\pi}{8}\right) \\
& \times ((-1)^{v_t} - (-1)^{v_{t-3}} - (-1)^{v_{t-4}} + (-1)^{v_{t-7}}) \\
& + \frac{1}{4}\left((2+\sqrt{2})^{t+\frac{1}{2}}\cos\frac{3\pi}{8} - (2-\sqrt{2})^{t+\frac{1}{2}}\cos\frac{\pi}{8}\right) \\
& \times ((-1)^{v_{t-1}} - (-1)^{v_{t-2}} - (-1)^{v_{t-5}} + (-1)^{v_{t-6}}).
\end{aligned}$$

With (5), we get

$$\begin{aligned}
& (2+\sqrt{2})^{t+\frac{1}{2}}\cos\frac{\pi}{8} + (2-\sqrt{2})^{t+\frac{1}{2}}\cos\frac{3\pi}{8} \\
& \quad = \frac{1}{2}\left((2+\sqrt{2})^{t+1} + (2-\sqrt{2})^{t+1}\right) \\
& \quad = D_{t+1}^+ \\
& \quad = 2D_t^+ + 2D_t^-
\end{aligned}$$

and

$$\begin{aligned}
& (2+\sqrt{2})^{t+\frac{1}{2}}\cos\frac{3\pi}{8} - (2-\sqrt{2})^{t+\frac{1}{2}}\cos\frac{\pi}{8} \\
& \quad = \frac{1}{\sqrt{2}}\left((2+\sqrt{2})^t - (2-\sqrt{2})^t\right) \\
& \quad = 2D_t^-.
\end{aligned}$$

Using (6), we finally deduce

$$\begin{aligned}\mathcal{F}(f) = &2^{2t-2}(A(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \\ &\quad + A(v_{t-1}, v_{t-6}, v_{t-2}, v_{t-5})) \\ &+ 2^{t-2}(A(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \\ &\quad - A(v_{t-1}, v_{t-6}, v_{t-2}, v_{t-5})) \\ &+ \frac{1}{2}D_t^+ B(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \\ &+ \frac{1}{2}D_t^- (B(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \\ &\quad + B(v_{t-1}, v_{t-6}, v_{t-2}, v_{t-5})).\end{aligned}$$

Now, we focus on the functions for which the previous quantity vanishes.

*Theorem 5:* For any odd $n \geq 3$, the only balanced symmetric Boolean functions of $n$ variables of degree less than or equal to 7 are the trivial balanced functions.

*Proof:* For any $f \in \mathcal{B}_n$ with $n = 2t+1$ and $\deg(f) \leq 7$, we have

$$\begin{aligned}\mathcal{F}(f) = &2^{2t-2}(A_1 + A_2) + 2^{t-2}(A_1 - A_2) \\ &+ \frac{1}{2}D_t^+ B_1 + \frac{1}{2}D_t^- (B_1 + B_2)\end{aligned}$$

where

$$\begin{cases} A_1 = A(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \\ B_1 = B(v_t, v_{t-7}, v_{t-3}, v_{t-4}) \end{cases}$$

and

$$\begin{cases} A_2 = A(v_{t-1}, v_{t-6}, v_{t-2}, v_{t-5}) \\ B_2 = B(v_{t-1}, v_{t-6}, v_{t-2}, v_{t-5}). \end{cases}$$

We have to distinguish the following cases.

- If $A_1 + A_2 \neq 0$, then $|A_1 + A_2| \geq 2$. It follows that either

  $$\mathcal{F}(f) \geq 2^{2t-1} - 2^{t+1} - 2D_t^+ - 4D_t^-$$

  or

  $$\mathcal{F}(f) \leq -2^{2t-1} + 2^{t+1} + 2D_t^+ + 4D_t^-.$$

  Using that for any $k > 0$, $D_k^+ + 2D_k^- = D_{k+1}^-$, we deduce that

  $$|\mathcal{F}(f)| \geq 2^{2t-1} - 2^{t+1} - 2D_{t+1}^- > 0$$

  for any $t \geq 13$ where the last inequality is derived from Lemma 2.
- If $A_1 + A_2 = 0$ and $A_1 \neq 0$, we have

  $$|\mathcal{F}(f)| \geq \left|\frac{1}{2}D_t^+ B_1 + \frac{1}{2}D_t^- (B_1 + B_2)\right| - 2^t.$$

  It follows from Lemma 2 that for $B_1 = 0$ and $B_2 \neq 0$

  $$|\mathcal{F}(f)| \geq D_t^- - 2^t > 0$$

  for any $t \geq 4$. For $B_1 = 0$ and $B_2 = 0$, we obviously have

  $$|\mathcal{F}(f)| \geq 2^t > 0.$$

  For $B_1 \neq 0$

  $$\begin{aligned}|\mathcal{F}(f)| &\geq \left(D_t^+ + D_t^-\right) - 2D_t^- - 2^t \\ &\geq D_{t-1}^+ - 2^t > 0\end{aligned}$$

  when $t \geq 3$.
- If $A_1 = A_2 = 0$, we have

  $$|\mathcal{F}(f)| = \left|\frac{1}{2}B_1\left(D_t^+ + D_t^-\right) + \frac{1}{2}B_2 D_t^-\right|.$$

  If $B_1 \neq 0$, we deduce that

  $$|\mathcal{F}(f)| \geq \left(D_t^+ + D_t^-\right) - 2D_t^- = D_{t-1}^+ > 0.$$

  If $B_1 = 0$, we obtain

  $$|\mathcal{F}(f)| = \frac{1}{2}|B_2| D_t^-$$

  which vanishes if and only if $B_2 = 0$.

Then, we have proved that for any odd $n \geq 27$, a symmetric function $f \in \mathcal{B}_n$ with $\deg(f) \leq 7$ is balanced if and only if $A_1 = A_2 = B_1 = B_2 = 0$. This situation occurs if and only if

$$\begin{cases} v_t \oplus v_{t-7} = 1 \\ v_{t-3} \oplus v_{t-4} = 1 \\ v_{t-1} \oplus v_{t-6} = 1 \\ v_{t-2} \oplus v_{t-5} = 1 \end{cases}$$

where $t = (n-1)/2$. This condition exactly corresponds to $v_i \oplus v_{2t+1-i} = 1$ for all $0 \leq i \leq 2t+1$. By computing all possible values of $\mathcal{F}(f)$ for the symmetric functions of $n$ variables when $n$ is odd and $3 \leq n < 27$, we finally check that the only balanced symmetric functions are the trivial balanced functions. □

Using both previous theorems which exhibit all balanced symmetric functions of degree at most 7, we can determine all symmetric functions of degree at most 8 which either satisfy $PC(1)$ or are 1-resilient. The functions satisfying $PC(1)$ are obtained by combining Theorems 4, 5, as well as Propositions 3 and 13.

*Corollary 5:* Let $f \in \mathcal{B}_n$, $n \geq 3$, be a symmetric function with $\deg(f) \leq 8$. Then, $f$ satisfies $PC(1)$ if and only if it satisfies one of the following conditions:

- $\deg(f) = 2$,
- $D_{\mathbf{1}} f$ has degree 1,
- $f$ is a 9-variable function of degree 8 defined by one of the eight following simplified ANF vectors:

  $$\lambda(f) = (\varepsilon_0, \varepsilon_1, 1, 1, 0, 0, 0, 0, 1, 0)$$
  $$\text{or } \lambda(f) = (\varepsilon_0, \varepsilon_1, 1, 1, 1, 0, 1, 0, 1, 0)$$

  with $\varepsilon_0, \varepsilon_1 \in \boldsymbol{F}_2$.

*Corollary 6:* Let $f \in \mathcal{B}_n$, $n \geq 3$, be a symmetric function with $\deg(f) \leq 7$. Then, $f$ is 1-resilient if and only if it has degree 1.

*Proof:* By definition, $f$ is 1-resilient if and only if it is balanced and the $(n-1)$-variable symmetric functions $f_H$ and $f_{e_n+H}$ corresponding to its restrictions to $H = \langle e_1, \ldots, e_{n-1}\rangle$ and to $e_n + H$ are balanced. If $n$ is even, $f_H$ and $f_{e_n+H}$ are balanced if and only if they are trivial balanced (Theorem 5). Then, Proposition 10 implies that $f$ has degree 1. If $n$ is odd and $\deg(f) \neq 1$, then either $f_H$ or $f_{e_n+H}$ is one of the 8-variable function with degree 7 defined in Theorem 4. It follows from Corollary 1 that $f$ is a 9-variable symmetric function of degree 7. It cannot be trivial balanced since $\deg(D_{\mathbf{1}}f) = \deg(f)-1 = 6$ (Proposition 15). □

## VII. Highly Nonlinear Symmetric Boolean Functions

The maximum nonlinearity for symmetric Booelan functions of $n$ variables has been proved to be reached only by quadratic functions. Precisely, when $n$ is even, then these functions are bent and the maximum nonlinearity is $2^{n-1}-2^{\frac{n}{2}-1}$[5] and when $n$ is odd, then the maximum nonlinearity is $2^{n-1} - 2^{\frac{n-1}{2}}$[6]. In this section , we investigate cases of suboptimal nonlinearity and we point out that the nonlinearity is related to the periodicity of the simplified value vector.

We recall the notation

$$\mathcal{L}(f) = \max_{a\in \boldsymbol{F}_2^n} |\mathcal{F}(f+\varphi_a)|.$$

*Theorem 6:* Let $f$ be a symmetric Boolean function of $n$ variables. If

$$\mathcal{L}(f) < 2^{\left\lfloor \frac{n+1}{2}\right\rfloor} + 2^{t+1}$$

for some integer $t$, $0 \leq t < \left\lfloor \frac{n-1}{2}\right\rfloor$, then

$$v_f(i+2) = v_f(i) \oplus 1, \qquad \text{for all } t \leq i \leq n-2-t$$

or equivalently, $f = q + h$ where $q$ is a symmetric quadratic function and $h$ is a symmetric function of $n$ variables such that $v_h(i) = 0$ for all $t \leq i \leq n-t$.

*Proof:* By induction on $t$.

- For $t = 0$. Suppose that

  $$\mathcal{L}(f) < 2^{\left\lfloor \frac{n+1}{2}\right\rfloor} + 2.$$

  Then, $\mathcal{L}(f) = 2^{\left\lfloor \frac{n+1}{2}\right\rfloor}$ since $\mathcal{L}(f)$ is an even integer. Therefore, it is known from [5], [6] that $f$ is quadratic and the expression of $v(f)$ is directly derived from Proposition 4.
- Induction step. Assume that

  $$\mathcal{L}(f) < 2^{\left\lfloor \frac{n+1}{2}\right\rfloor} + 2^{t+1}.$$

  Let $f_{\bar{H}}$ be the restriction of $f$ to the affine subspace $\bar{H} = \{x \in \boldsymbol{F}_2^n,\ x_{n-1} + x_n = 1\}$. We have from [10, Corollary V.3] that $\mathcal{L}(f) \geq \mathcal{L}(f_{\bar{H}})$. Moreover, with the notation of Proposition 7, $f_{\bar{H}}$ can be written as

  $$f_{\bar{H}}(x_1, \ldots, x_{n-1}) = (1+x_{n-1})f_{e_n+V} + x_{n-1}f_{e_{n-1}+V}$$

  where $V = \langle e_1, \ldots e_{n-2}\rangle$. But, we know from Proposition 7 that $f_{e_n+V} = f_{e_{n-1}+V}$ and that this function is a symmetric function of $(n-2)$ variables. Let $g = f_{e_n+V} = f_{e_{n-1}+V}$. Since

  $$f_{\bar{H}}(x_1, \ldots, x_{n-1}) = g(x_1, \ldots, x_{n-2})$$

  we have $\mathcal{L}(f_{\bar{H}}) = 2\mathcal{L}(g)$. Therefore, $g$ is an $(n-2)$-variable symmetric function which satisfies

  $$\mathcal{L}(g) < 2^{\left\lfloor \frac{(n-2)+1}{2}\right\rfloor} + 2^t.$$

  By induction hypothesis, we deduce that $v_g(i+2) = v_g(i) \oplus 1$ for all $i$ such that $t-1 \leq i \leq (n-2)+1-t$. However, the simplified value vector of $g$ is related to the simplified value vector of $f$ by $v_g(i) = v_f(i+1)$ for all $0 \leq i \leq n-2$ (see Proposition 7). It follows that, for all $t \leq i \leq n-2-t$

  $$v_f(i+2) = v_g(i+1) = v_g(i-1) \oplus 1 = v_f(i) \oplus 1. \quad \square$$

As a direct corollary, we can deduce a necessary condition on the simplified value vector of the symmetric functions $f$ with

$$\mathcal{L}(f) < 2^{\frac{n}{2}+1}, \qquad \text{if } n \text{ is even}$$
$$\mathcal{L}(f) < 2^{\frac{n+1}{2}} + 2^{\frac{n-1}{2}}, \qquad \text{if } n \text{ is odd.}$$

*Corollary 7:* Let $f$ be a symmetric function of $n$ variables.

- For $n$ even, if $v_f\left(\frac{n}{2}-1\right) = v_f\left(\frac{n}{2}+1\right)$, then $\mathcal{L}(f) \geq 2^{\frac{n+1}{2}} + 2^{\frac{n-1}{2}}$.
- For $n$ odd, if $v_f\left(\frac{n+1}{2}\right) = v_f\left(\frac{n-3}{2}\right)$ or if $v_f\left(\frac{n+3}{2}\right) = v_f\left(\frac{n-1}{2}\right)$, then $\mathcal{L}(f) \geq 2^{\frac{n+1}{2}} + 2^{\frac{n-1}{2}}$.

Theorem 6 also points out that the resiliency order of a highly nonlinear symmetric function is limited.

*Corollary 8:* Let $f$ be a symmetric function of $n$ variables such that

$$\mathcal{L}(f) < 2^{\left\lfloor \frac{n+1}{2}\right\rfloor} + 2^{t+1}$$

for some integer $t$, $0 \leq t < \left\lfloor \frac{n-1}{2}\right\rfloor$. Then, $f$ is at most $(2t+2)$-resilient.

*Proof:* Let $g$ denote its restriction to $\langle e_1, \ldots, e_{n-t}\rangle$. From Proposition 7, $g$ is a symmetric function of $(n-t)$ variables and its simplified value vector is given by $v_g(i) = v_f(i)$ for all $0 \leq i \leq n-t$. Therefore, $v(g)$ is ultimately periodic with period 4 and pre-period $t$. Moreover, $g$ is not linear since $v_g(t+2) = v_g(t) \oplus 1$. We deduce from Corollary 2 that the resiliency order of $g$ is at most $t+2$, implying that $f$ is at most $(2t+2)$-resilient. □

Now, we can characterize the symmetric functions whose nonlinearity is very close to the optimal nonlinearity. Here, we use the following lemma which shows how the Walsh spectrum of such a function can be computed from the Walsh spectrum of a quadratic function.

*Lemma 3:* Let $f$ be a symmetric function of $n$ variables such that

$$\mathcal{L}(f) < 2^{\left\lfloor \frac{n+1}{2}\right\rfloor} + 2^{t+1}$$

for some integer $t$, $0 \leq t < \lfloor \frac{n-1}{2} \rfloor$. Then, there exists a symmetric quadratic function $q \in \mathcal{B}_n$ such that, for any $\alpha \in \boldsymbol{F}_2^n$ of weight $w$

$$\mathcal{F}(f+\varphi_\alpha) = \mathcal{F}(q+\varphi_\alpha) - 2\sum_{i=0}^{t-1} \left( h_i(-1)^{v_q(i)} + h_{n-i}(-1)^{v_q(n-i)\oplus w} \right) P_i(w)$$

where $h_i = v_f(i) \oplus v_q(i)$, $i \in \{0, \ldots t-1\} \cup \{n-t+1, \ldots, n\}$, and $P_i$ is the Krawtchouk polynomial of degree $i$ as defined in Proposition 3.

*Proof:* Theorem 6 implies that $f = q + h$ where $q$ is a quadratic symmetric function and $h$ is a symmetric function such that $v_h(i) = 0$ for all $t \leq i \leq n - t$. Let $h_i = v_h(i)$. From Proposition 3, for any $\alpha \in \boldsymbol{F}_2^n$ of weight $w$, the Walsh coefficients of $f$ are given by

$$\mathcal{F}(f+\varphi_\alpha) = \sum_{i=0}^{n} (-1)^{v_f(i)} P_i(w).$$

Using that $(-1)^{v_f(i)} = (-1)^{v_q(i)}(-1)^{h_i} = (-1)^{v_q(i)}(1-2h_i)$, we deduce that

$$\mathcal{F}(f+\varphi_\alpha) = \mathcal{F}(q+\varphi_\alpha) - 2\left( \sum_{i=0}^{t-1} (-1)^{v_q(i)} h_i P_i(w) + \sum_{i=n-t+1}^{n} (-1)^{v_q(i)} h_i P_i(w) \right)$$

and the result comes directly from the fact that $P_{n-i}(w) = (-1)^w P_i(w)$ for any integer $w$. □

*Proposition 20:* The symmetric functions $f$ of $n$ variables such that

$$\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 2$$

are the eight functions of degree $n$ defined by the following simplified ANF vectors:

$$\lambda_f = (a, b, 1, 0, \ldots, 0, 1) \quad \text{and} \quad \lambda_f = (a, b, 0, 1, \ldots, 1, 1), \quad a, b \in \boldsymbol{F}_2.$$

*Proof:* From Theorem 6, $f = q + h$ where $q$ is a quadratic symmetric function and $h$ is a symmetric function such that $v(h) = (h_0, 0, \ldots, 0, h_n)$. Therefore, the simplified ANF vector of $h$ is

$$\lambda_h = (h_0, h_0, \ldots, h_0, h_0 \oplus h_n).$$

It is well known that $\mathcal{L}(f)$ is not divisible by 4 if and only if $f$ has degree $n$ (since its Hamming weight is odd). Then, we must have $h_0 \oplus h_n = 1$. For $h_0 = 1$ and $h_n = 0$, we have from the previous lemma that, for any $\alpha$ of weight $w$

$$\mathcal{F}(f+\varphi_\alpha) = \mathcal{F}(q+\varphi_\alpha) - 2(-1)^{v_q(0)}.$$

We deduce from Proposition 16 that, for any function $f$ with $\lambda_f = (a, b, 0, 1, \ldots, 1, 1)$, the set $\{|\mathcal{F}(f+\varphi_\alpha), \alpha \in \boldsymbol{F}_2^n\}$ equals $\{2^{\frac{n}{2}} - 2, 2^{\frac{n}{2}} + 2\}$ when $n$ is even and $\{2^{\frac{n+1}{2}} - 2, 2^{\frac{n+1}{2}} + 2, 2\}$ when $n$ is odd.

Similarly, for $h_0 = 0$ and $h_n = 1$, we have

$$\mathcal{F}(f+\varphi_\alpha) = \mathcal{F}(q+\varphi_\alpha) - 2(-1)^{v_q(n)\oplus w}.$$

Then, for any function $f$ with $\lambda_f = (a, b, 1, 0, \ldots, 0, 1)$, the set $\{|\mathcal{F}(f+\varphi_\alpha)|, \alpha \in \boldsymbol{F}_2^n\}$ equals $\{2^{\frac{n}{2}} - 2, 2^{\frac{n}{2}} + 2\}$ when $n$ is even and $\{2^{\frac{n+1}{2}} - 2, 2^{\frac{n+1}{2}} + 2, 2\}$ when $n$ is odd. □

*Proposition 21:* The symmetric functions $f$ of $n$ variables such that

$$\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 4$$

are the four functions of degree $(n-1)$ defined by the following simplified ANF vectors:

$$\lambda_f = (a, b, 0, 1, \ldots, 1, 0), \qquad a, b \in \boldsymbol{F}_2.$$

*Proof:* From Theorem 6, $f = q + h$ where $q$ is a quadratic symmetric function and $h$ is a symmetric function such that $v(h) = (h_0, h_1, 0, \ldots, 0, h_{n-1}, h_n)$. From the previous lemma, we have, for any $\alpha$ of weight $w$

$$\begin{aligned}\mathcal{F}(f+\varphi_\alpha) &= \mathcal{F}(q+\varphi_\alpha) - 2\left( h_0(-1)^{v_q(0)} + h_n(-1)^{v_q(n)+w} \right) \\ &\quad - 2(n-2w)\left( h_1(-1)^{v_q(1)} + h_{n-1}(-1)^{v_q(n-1)+w} \right).\end{aligned}$$

Clearly, we have

$$\left| h_0(-1)^{v_q(0)} + h_n(-1)^{v_q(n)+w} \right| \leq 2.$$

Therefore,

$$|\mathcal{F}(f+\varphi_\alpha)| \geq \Big| \mathcal{F}(q+\varphi_\alpha) - 2(n-2w) \left( h_1(-1)^{v_q(1)} + h_{n-1}(-1)^{v_q(n-1)+w} \right) \Big| - 4.$$

If $(h_1, h_{n-1}) \neq (0, 0)$, we have

$$h_1(-1)^{v_q(1)} + h_{n-1}(-1)^{v_q(n-1)+w} \in \{(-1)^{v_q(1)}, 2(-1)^{v_q(1)}\}$$

for $w \equiv v_q(1) \oplus v_q(n-1) \bmod 2$.

However, we can check from Proposition 16 that, when $\alpha$ varies in the set of all elements such that

$$\mathrm{wt}(\alpha) \equiv v_q(1) \oplus v_q(n-1) \bmod 2$$

$\mathcal{F}(q+\varphi_\alpha)$ takes both values $\pm 2^{\lfloor \frac{n+1}{2} \rfloor}$. Therefore, there always exists an $\alpha$ with $\mathrm{wt}(\alpha) = w \leq 3$ such that

$$\mathcal{F}(q+\varphi_\alpha) = (-1)^{v_q(1)+1} 2^{\lfloor \frac{n+1}{2} \rfloor}$$

implying that

$$\left| \mathcal{F}(q+\varphi_\alpha) - 2(n-2w)\left( h_1(-1)^{v_q(1)} + h_{n-1}(-1)^{v_q(n-1)+w} \right) \right| \geq 2^{\lfloor \frac{n+1}{2} \rfloor} + 2(n-2w).$$

TABLE IV
WALSH COEFFICIENTS OF SYMMETRIC BOOLEAN FUNCTIONS OF NONLINEARITY $2^{n-1} - 2^{\lfloor \frac{n-1}{2} \rfloor} - 2$ WITH A NULL CONSTANT TERM

| $\mathcal{F}(f+\varphi_\alpha)$ | $n \equiv 0 \bmod 4$ | $n \equiv 2 \bmod 4$ | $n \equiv 1 \bmod 4$ | $n \equiv 3 \bmod 4$ |
|---|---|---|---|---|
| $wt(\alpha) \equiv 0 \bmod 4$ | $(-1)^{\frac{n}{4}} 2^{\frac{n}{2}} - 4$ | $(-1)^{\lambda}(-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}}$ | $((-1)^{\lambda}+1)$ $\left((-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}} - 2\right)$ | $((-1)^{\lambda+1}+1)$ $\left((-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}} - 2\right)$ |
| $wt(\alpha) \equiv 1 \bmod 4$ | $(-1)^{\lambda+1}(-1)^{\frac{n}{4}} 2^{\frac{n}{2}}$ | $(-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}} - 4$ | $((-1)^{\lambda+1}+1)$ $\left((-1)^{\frac{n-1}{4}} 2^{\frac{n-1}{2}} - 2\right)$ | $((-1)^{\lambda}+1)$ $\left((-1)^{\frac{n-3}{4}} 2^{\frac{n-1}{2}} - 2\right)$ |
| $wt(\alpha) \equiv 2 \bmod 4$ | $(-1)^{\frac{n}{4}+1} 2^{\frac{n}{2}} - 4$ | $(-1)^{\lambda+1}(-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}}$ | $((-1)^{\lambda}+1)$ $\left((-1)^{\frac{n+3}{4}} 2^{\frac{n-1}{2}} - 2\right)$ | $((-1)^{\lambda+1}+1)$ $\left((-1)^{\frac{n-3}{4}} 2^{\frac{n-1}{2}} - 2\right)$ |
| $wt(\alpha) \equiv 3 \bmod 4$ | $(-1)^{\lambda}(-1)^{\frac{n}{4}} 2^{\frac{n}{2}}$ | $(-1)^{\frac{n-2}{4}+1} 2^{\frac{n}{2}} - 4$ | $((-1)^{\lambda+1}+1)$ $\left((-1)^{\frac{n+3}{4}} 2^{\frac{n-1}{2}} - 2\right)$ | $((-1)^{\lambda}+1)$ $\left((-1)^{\frac{n+1}{4}} 2^{\frac{n-1}{2}} - 2\right)$ |

It follows that, for any choice of $(h_0, h_n)$, there exists an $\alpha$ with $\mathrm{wt}(\alpha) = w \leq 3$ such that

$$\begin{aligned} |\mathcal{F}(f+\varphi_\alpha)| &\geq 2^{\lfloor \frac{n+1}{2} \rfloor} + 2(n-2w) - 4 \\ &\geq 2^{\lfloor \frac{n+1}{2} \rfloor} + 2n - 16 \\ &> 2^{\lfloor \frac{n+1}{2} \rfloor} + 4 \end{aligned}$$

when $n > 10$. We then deduce that both $h_1$ and $h_{n-1}$ must be 0 if $\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 4$ when $n > 10$ and we checked by computer that this condition also holds when $n \leq 10$. Therefore, the simplified ANF vector of $h$ is

$$\lambda_h = (h_0, h_0, \ldots, h_0, h_0 \oplus h_n)$$

and we must have $h_0 = h_n = 1$—otherwise $\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 2$. In this case

$$\mathcal{F}(f+\varphi_\alpha) = \mathcal{F}(q+\varphi_\alpha) - 2\left((-1)^{v_q(0)} + (-1)^{v_q(n)+w}\right).$$

If we consider the quadratic Boolean functions with simplified ANF vector $\lambda(q) = (0, \lambda, 1, 0, \ldots, 0)$, $\lambda \in \boldsymbol{F}_2$, then $v_q(0) = 0$ and $v_q(n)$ depends on the value of $n \bmod 4$

$$v_q(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod 4 \\ 1, & \text{if } n \equiv 2 \bmod 4 \\ \lambda, & \text{if } n \equiv 1 \bmod 4 \\ \lambda \oplus 1, & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

We can compute the value of

$$\mathcal{F}(q+\varphi_\alpha) - 2\left(1 + (-1)^{v_q(n)+\mathrm{wt}(\alpha)}\right)$$

that we present in Table IV.

The case where $v_q(0) = 1$ is straightforward as we get $-\mathcal{F}(f+\varphi_\alpha)$. Then, for any function $f$ with $\lambda_f = (a, b, 0, 1, \ldots, 1, 0)$, the set

$$\{|\mathcal{F}(f+\varphi_\alpha)|, \alpha \in \boldsymbol{F}_2^n\}$$

equals $\{2^{\frac{n}{2}}, 2^{\frac{n}{2}} - 4, 2^{\frac{n}{2}} + 4\}$ when $n$ is even and $\{2^{\frac{n+1}{2}} + 4, 2^{\frac{n+1}{2}} - 4, 0\}$ when $n$ is odd. □

## VIII. CONCLUSION

Our study points out that the symmetry property combined with some cryptographic requirements, such as a high algebraic degree, a high degree of propagation, or a high order of resiliency, can only be achieved by functions having a very regular representation. For instance, we proved that any symmetric function of degree $d$ can be described by the representation of a $(2^{\lfloor \log_2 d \rfloor + 1} - 1)$-variable symmetric function repeated periodically. Such regularities considerably reduce the number of symmetric functions which may be optimal with respect to some cryptographic parameters. It confirms, for other criteria, the results obtained by Savicky [5] and by Maitra and Sarkar [6] on maximally nonlinear symmetric functions. As an illustration of this situation, we proved that balanced symmetric functions of degree less than or equal to 7 (excluding the trivial cases) only exist for eight variables. The very small number of nontrivial balanced functions seems to be the main obstacle to the existence of highly resilient symmetric functions. We actually conjecture that balanced symmetric functions of fixed degree do not exist when the number of variables grows. However, the generalization of the technique we used for functions of degree at most 7 remains open.

## ACKNOWLEDGMENT

The authors would like to thank Pascale Charpin for valuable discussions, comments, and suggestions all along this work.

## REFERENCES

[1] I. Wegener, *The Complexity of Boolean Functions*. New York: Wiley, 1987.
[2] J. O. Brüer, "On pseudorandom sequences as crypto generators," in *Proc. 1984 Int. Zürich Seminar on Digital Communications*, Zürich, Switzerland, 1984, pp. 157–161.
[3] C. J. Mitchell, "Enumerating Boolean functions of cryptographic significance," *J. Cryptol.*, vol. 2, no. 3, pp. 155–170, 1990.
[4] B. Guo and X. Yang, "Further enumerating Boolean functions of cryptographic significance," *J. Cryptol.*, vol. 8, no. 3, pp. 115–122, 1995.
[5] P. Savicky, "On the bent Boolean functions that are symmetric," *Europ. J. Combin.*, vol. 15, pp. 407–410, 1994.
[6] S. Maitra and P. Sarkar, "Maximum nonlinearity of symmetric Boolean functions on odd number of variables," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2626–2630, Sep. 2002.
[7] K. Gopalakrishnan, D. Hoffman, and D. Stinson, "A note on a conjecture concerning symmetric resilient functions," *Inform. Process. Lett.*, vol. 47, no. 3, pp. 139–143, 1993.
[8] J. von zur Gathen and J. Roche, "Polynomials with two values," *Combinatorica*, vol. 17, no. 3, pp. 345–362, 1997.
[9] P. Sarkar and S. Maitra, "Balancedness and correlation immunity of symmetric Boolean functions," in *Proc. R. C. Bose Centenary Symp.*, vol. 15, 2003, pp. 178–183.

[10] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1, m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1494–1513, May 2001.

[11] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Adv. Cryptology—EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 386–397.

[12] O. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.

[13] L. Comtet, *Advanced Combinatorics*. Amsterdam, The Netherlands: Reidel, 1974.

[14] E. Dawson and C. Wu, "On the linear structure of symmetric Boolean functions," *Australas. J. Comb.*, vol. 16, pp. 239–243, 1997.

[15] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[16] B. Preneel, W. Leekwijck, L. Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Adv. Cryptology—EUROCRYPT'90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 437, pp. 155–165.

[17] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Adv. Cryptology—EUROCRYPT'89 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1990, vol. 434, pp. 549–562.

[18] A. Gouget, "On the propagation criterion of Boolean functions," in *Coding, Cryptography and Combinatorics*. ser. Progr. Comput. Sci. Appl. Logic, C. X. K. Feng and H. Niederreiter, Eds. Basel, Switzerland: Birkhäuser-Verlag, 2004, vol. 23.

[19] J. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Univ. Maryland, College Park, MD, 1974.